Indústria de pagamento de cartão (PCI)

Padrão de dados do aplicativo de pagamento

Requisitos e procedimentos de avaliação de segurança

Versão 2.0

Outubro de 2010

Alterações do documento

Data	Versão	Descrição	Páginas
1º de outubro de 2008	*1.2*	*Para alinhar o conteúdo com o novo PCI DSS v1.2 e para implementar alterações menores observadas desde o original v1.1.*	
Julho de 2009	*1.2.1*	*Em "Escopo do PA-DSS", alinhe o conteúdo com o* Guia do programa PA-DSS, v 1.2.1 *para esclarecer em que casos o PA-DSS é aplicável.*	*v, vi*
		Sob o Requisito de laboratório 6, a escrita correta de "OWASP".	*30*
		No atestado de validação, Parte 2a, atualize a funcionalidade de aplicativo de pagamento para que esteja consistente com os tipos de aplicação listadas no Guia de programa PA-DSS *e esclareça os procedimentos anuais de revalidação na Parte 3b.*	*32, 33*
Outubro de 2010	*2.0*	*Atualize e implemente alterações menores da versão 1.2.1 e alinhe-a com o novo PCI DSS versão 2.0. Para obter detalhes, consulte* "PA-DSS—Resumo das alterações do PA-DSS Versão 1.2.1 para 2.0.*"*	

Índice

Introdução

Propósito deste documento

Este documento deve ser usado pelos Avaliadores de segurança qualificados do aplicativo de pagamento (PA-QSAs) ao conduzir revisões no aplicativo de pagamento, para que os fornecedores do software possam validar que o aplicativo de pagamento está de acordo com o Padrão de segurança de dados do aplicativo de pagamento PCI (PA-DSS). Este documento também deve ser usado para os PA-QSAs como modelo para criar o Relatório na Validação.

Recursos adicionais, incluindo Atestados de validação, Perguntas frequentes (FAQs) e o *Glossário de termos, abreviações e acrônimos PCI DSS e PA-DSS* estão disponíveis no site do Conselho de padrões de segurança PCI (PCI SSC) —www.pcisecuritystandards.org.

Relação entre PCI DSS e PA-DSS

O uso de um aplicativo em conformidade com o PA-DSS por si só não torna a entidade compatível com PCI DSS, já que o aplicativo deve ser implementar em um ambiente compatível com PCI DSS e de acordo com o Guia de Implementação PA-DSS fornecido pelo fornecedor do aplicativo de pagamento (por Requisito do PA-DSS 13.1)

Os requisitos do Padrão de segurança de dados do aplicativo de pagamento (PA-DSS) são derivados dos *Procedimentos de avaliação de segurança e requisitos do padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS)*. Este documento, que pode ser encontrado em www.pcisecuritystandards.org, detalha o que é necessário para estar de acordo com o PCI DSS (e, portanto, o que um aplicativo de pagamento devem apoiar para facilitar a conformidade do cliente com PCI DSS).

A conformidade tradicional com o Padrão de segurança de dados PCI pode não aplicar-se diretamente aos fornecedores do aplicativo de pagamento, já que a maioria dos fornecedor não armazena, processa ou transmite dados do proprietário do cartão. No entanto, já que esses aplicativos de pagamento são usados pelos cliente para armazenar, processar e transmitir dados do proprietário do cartão e os clientes devem estar em conformidade com o Padrão de segurança de dados PCI, os aplicativos de pagamento devem facilitar, e não evitar, estar em conformidade com o Padrão de segurança de dados PC do cliente. Seguem apenas algumas maneiras de como é possível para os aplicativos de pagamento evitar a conformidade.

1. O armazenamento de dados na faixa magnética e/ou dados equivalentes no chip da rede do cliente após autorização;
2. Os aplicativos que necessitam de cliente devem desabilitar outros recursos requisitados pelo Padrão de segurança de dados PCI, como softwares antivírus ou firewalls, para fazer com que o aplicativo de pagamento funcione adequadamente; e
3. Os uso dos fornecedores de métodos inseguros para conectar-se ao aplicativo para fornecer suporte ao cliente.

Os aplicativos de pagamento seguro, quando implementados em um ambiente em conformidade com PCI DSS, minimizará o potencial de brechas na segurança, o que leva ao comprometimento de dados em faixas magnéticos totais, códigos de verificação de cartão e valores (CAV2, CID, CVC2, CVV2), PINs e bloqueios de PIN e fraude, resultando em brechas.

Escopo do PA-DSS.

O PA-DSS aplica-se aos fornecedores de software e outro que desenvolvem aplicativos de pagamento que armazenam, processam ou transmitem dados do proprietário do cartão como parte da autorização ou determinação, casos em que os aplicativos de pagamento são vendidos, distribuídos ou licenciados a terceiros.

O guia a seguir pode ser usado para determinar se o PA-DSS aplica-se a um determinado aplicativo do pagamento:

> ***Observação:***
> *Todos os produtos do aplicativo de pagamento validados não devem ser versão beta.*

- O PA-DSS aplica-se aos aplicativos de pagamento que normalmente são vendidos e instalados do modo como vieram, sem muita personalização pelos fornecedores de software.
- O PA-DSS não aplica-se aos aplicativos de pagamento fornecidos em módulos, o que normalmente inclui um módulo de "linha de base" e outros módulos específicos dos tipos e funções do cliente ou personalizados por solicitação do cliente. O PA-DSS pode aplicar-se apenas ao módulo de linha de base se o módulo for o único realizando funções de pagamento (uma vez confirmado por PA-QSA). Se outros módulos também realizarem funções de pagamento, o PA-DSS aplica-se a esses módulos também. Observe que é considerado uma boa prática que os fornecedores do software isolem as funções de pagamento em uma quantidade pequena de módulos de linha de base, reservando outros módulos para funções de não pagamento. Esta boa prática (embora não seja um requisito) pode limitar o número de módulos sujeitos ao PA-DSS.
- O PA-DSS NÃO aplica-se aos aplicativos de pagamento oferecidos pelos fornecedores de aplicativos ou serviço apenas como serviço (a menos que tais aplicativos também sejam vendidos, licenciados ou distribuídos a terceiros) porque:

  1) O aplicativo é um serviço oferecido aos clientes (normalmente comerciantes), que não têm a habilidade de gerenciar, instalar ou controlar o aplicativo ou seu ambiente;
  2) O aplicativo é coberto pela revisão PCI DSS do próprio fornecedor do aplicativo ou do serviço (essa cobertura deve ser confirmada pelo cliente); e/ou
  3) O aplicativo não é vendido, distribuído ou licenciado a terceiros.

  Exemplos destes aplicativos de pagamento de "software como serviço" incluem:

  1) Os aplicativos oferecidos por Fornecedores de serviço de aplicativo (ASP) que hospedam um aplicativo de pagamento no site para uso do cliente. Observe que o PA-DSS pode aplicar-se, no entanto, se o aplicativo de pagamento do ASP for também vendido para um site de terceiros e implementado e o aplicativo não foi coberto pela revisão PCI DSS do ASP.
  2) Os aplicativos terminais virtuais que estão no site do provedor de serviço e são usados pelos comerciantes para inserir as transações de pagamento. Observe que o PA-DSS se aplicaria se o aplicativo terminal virtual tivesse uma parte distribuída para o site do comerciante e fosse implementada nele e não fosse coberta pela revisão PCI DSS do fornecedor terminal virtual.

- O PA-DSS NÃO aplica-se a aplicativos que não sejam de pagamento que façam parte do conjunto de aplicativos de pagamento. Tais aplicativos (por exemplo, aplicativo de monitoração de fraude, pontuação ou detecção incluído no conjunto) podem ser, mas não é obrigatório, cobertos pelo PA-DSS se todo o conjunto for avaliado junto. No entanto, se o aplicativo de pagamento for parte de um conjunto que baseia-se nos requisitos do PA-DSS sendo atingidos pelos controles em outros aplicativos do conjunto, deve-se realizar uma única avaliação PA-DSS do aplicativo de pagamento e todos os outros aplicativos do conjunto no qual se baseia. Os aplicativos não

devem ser avaliadas separadamente dos aplicativos em que se baseiam, já que todos os requisitos do PA-DSS não são preenchidos em um único aplicativo.

- O PA-DSS NÃO se aplica a aplicativos de pagamento desenvolvidos e vendidos para um único cliente para uso exclusivo dele, já que este aplicativo será coberto como parte da revisão de conformidade PCI DSS normal do cliente. Observe que o aplicativo (que pode ser referido como o aplicativo "já mencionado") é vendido para apenas um cliente (normalmente um comerciante grande ou provedor de serviço) e foi desenvolvido de acordo com as especificações fornecidas pelo cliente.
- O PA-DSS NÃO aplica-se a aplicativos de pagamento desenvolvidos por comerciantes e fornecedores de serviço se forem usados apenas internamente (não vendidos, distribuídos ou licenciados para terceiros), já que o aplicativo de pagamento desenvolvido internamente seria coberto como parte da conformidade PCI DSS normal do provedor de serviço.

Por exemplo, para os últimos dois tópicos acima, se os lugares que vendem o aplicativo de pagamento desenvolvido internamente ou "já mencionado" proíbem a autenticação sensível de dados ou permitem senhas complexas, serão cobertos como parte dos esforços de conformidade PCI DSS normais do comerciante ou do provedor de serviço e não requerem uma avaliação PA-DSS separada.

A lista a seguir, embora não inclua tudo, ilustra os aplicativos que NÃO são aplicativos de pagamento para fins de PA-DSS (e portanto não precisam passar por revisões PA-DSS):

- Sistemas operacionais em que o aplicativo de pagamento esteja instalado (por exemplo, Windows Unix)
- Sistemas de banco de dados que armazenam dados do proprietário do cartão (por exemplo, Oracle)
- Sistemas de back office que armazenam dados do proprietário do cartão (por exemplo, para fins de relatórios ou de serviço ao cliente)

Observação: *O PCI SSC lista APENAS aplicativos de pagamento.*

O escopo da revisão PA-DSS deve incluir o seguinte:

- Cobertura de todas as funcionalidade do aplicativo de pagamento, incluindo, mas não limitando-se a 1) funções de pagamento de ponta a ponta (autorização e definição), 2) entrada e saída, 3) condições de erro, 4) interfaces e conexões com outros arquivos, sistemas e/ou aplicativos de pagamento ou componentes do aplicativo, 5) todos os fluxos de dados do proprietário do cartão, 6) mecanismos de criptografia e 7) mecanismos de autenticação.
- A cobertura da orientação do fornecedor do aplicativo de pagamento deve fornecer aos cliente e revendedores/integradores (consulte *Guia de Implementação PA-DSS* mais à frente neste documento) para garantir que 1) o cliente saiba como implementar o aplicativo de pagamento de uma maneira compatível com o PCI-DSS e que 2) o cliente seja avisado com clareza de que alguns aplicativos de pagamento e configurações de ambiente podem impedir a conformidade PCI DSS. Observe que o fornecedor do aplicativo de pagamento deve fornecer orientação para que mesmo quando a configuração específica 1) não possa ser controlada pelo fornecedor do aplicativo de pagamento, já que o aplicativo foi instalado pelo cliente ou 2) seja de responsabilidade do cliente, não do fornecedor de aplicativo de pagamento.
- Cobertura de todas as plataformas selecionada para a versão do aplicativo de pagamento revisado (as plataformas incluídas devem ser especificadas).
- Cobertura das ferramentas usadas pelo aplicativo de pagamento para acessar e/ou visualizar os dados do proprietário do cartão (ferramentas de relatório, ferramentas de registro, etc)

PA-DSS Aplicabilidade aos aplicativos de pagamento em terminais de hardware

Aplicativos de pagamento desenvolvidos para operar em terminais de hardware (também conhecidos como terminais independentes ou POS dedicados) podem passar por revisão PA-DSS se o fornecedor desejar alcançar a validação e se os requisitos de conformidade do PA-DSS puderem ser atendidos. As razões pelas quais o fornecedor pode desejar passar um aplicativo de pagamento pela validação PA-DSS no terminal de hardware incluem, mas não limitam-se a necessidades de negócios e obrigação de conformidade. Esta seção fornece orientação para os fornecedores que desejam obter validação PA-DSS para aplicações de pagamento residentes em terminais de hardware.

Há duas maneiras de o aplicativo de pagamento residente no terminal de hardware alcançar a validação PA-DSS:

1. O aplicativo de pagamento residente atende diretamente todos os requisitos do PA-DSS e é validado de acordo com os procedimento PA-DSS.
2. O aplicativo de pagamento residente não atende todos os requisitos do PA-DSS, mas o hardware onde reside o aplicativo é listado na Lista de dispositivos de segurança de transação PIN aprovados (PTS) do PCI SSC como dispositivo de Ponto de interação (POI) atualmente aprovado pelo PCI PTS. Neste cenário, pode ser possível que o aplicativo satisfaça os requisitos do PA-DSS através de uma combinação dos controles validades PA-DSS e PTS.

O resto dessa seção aplica-se apenas aos aplicativos de pagamento que residem em um dispositivo POI aprovado PCI PTS validado.

Se um ou mais requisitos do PA-DSS não forem atendidos diretamente pelo aplicativo de pagamento, eles podem ser atendidos indiretamente pelos controles estados como parte da validação PCI PTS. Para que um dispositivo de hardware seja considerado para inclusão em uma revisão PA-DSS, o dispositivo de hardware DEVE ser validado como dispositivo POI aprovado PCI PTS e incluído na Lista de dispositivos PTS aprovados PCI SSC. O dispositivo POI validado PTS, que fornece um ambiente de computação confiável, se tornará uma "***dependência necessária***" para o aplicativo do pagamento e a combinação do aplicativo e do hardware será incluída na Lista de aplicativos de pagamento validados PA-DSS.

Ao conduzir a avaliação PA-DSS, o PA-QSA deve testar totalmente o aplicativo de pagamento com seu hardware dependente em comparação com todos os requisitos do PA-DSS. Se o PA-QSA determina que um ou mais requisitos do PA-DSS não podem ser atendidos pelo aplicativo de pagamento residente, mas são atendidos por controles validados no PCI PTS, o PA-QSA deve:

1. Documentar claramente quais requisitos são atendidos conforme declarado pelo PA-DSS (como sempre);
2. Documentar claramente quais requisitos foram atendidos através do PCI PTS na caixa "Em funcionamento" para este requisito;
3. Incluir uma explicação completa de por que o aplicativo de pagamento não pode atender o requisito do PA-DSS;
4. Documente os procedimentos conduzidos para determinar como o requisito foi totalmente atendido através do controle validado PCI PTS;
5. Liste o terminal de hardware validade PCI PTS como dependência requisitada na Resumo executivo do relatório de validação.

Uma vez que a validação do PA-QSA do aplicativo de pagamento esteja concluída e, subsequentemente, aceita pelo PCI SSC, o o dispositivo de hardware validado PTS será listado como dependência para o aplicativo de pagamento na Lista de aplicativos validados PA-DSS.

Os aplicativos de pagamento residentes em terminais de hardware que são validados através de uma combinação de controles PA-DSS e PCI PTS devem atender os seguintes critérios:

1. Forneça juntamente para o cliente (terminal de hardwawre e aplicativo) OU, se fornecido separadamente, o fornecedor de aplicativo e/ou o revendedor/integrador deve empacotar o aplicativo para distribuição de forma que opere apenas no terminal de hardware em que foi validado para executar.
2. Ativado por padrão para suporte da conformidade PCI DSS do cliente.
3. Inclui suporte contínuo e atualizações para manter a conformidade PCI DSS.
4. Se o aplicativo for vendido separadamente, distribuído ou licenciado para clientes, o fornecedor deve fornecer detalhes do hardware dependente requisitado para o uso com o aplicativo, de acordo com a listagem de validação PA-DSS.

Funções e responsabilidades

Há várias partes interessadas na comunidade de aplicativos de pagamento. Algumas dessas partes interessadas têm uma participação mais direta no processo de avaliação PA-DSS - fornecedores, PA-QSAs e PSI SSC. Outras partes interessadas que não estão diretamente envolvidas com o processo de avaliação devem estar conscientes do processo geral para facilitar suas decisões de negócios associadas.

A seguir, são definidas as funções e responsabilidades das partes interessadas na comunidade de aplicativos de pagamento. Estas partes interessadas envolvidas no processo de avaliação têm as responsabilidades relacionadas listadas.

Marcas de pagamento

American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. são as marcas de pagamento que fundaram o PCI SSC. Essas marcas de pagamento são responsáveis pelo desenvolvimento e no reforço de programas relacionados com a conformidade PA-DSS, incluindo, mas não limitando-se, ao seguinte:

- Qualquer requisito, mandato ou data para uso dos aplicativos de pagamento em conformidade com PA-DSS.
- Qualquer multa ou penalidade relacionada ao uso de aplicativos de pagamento que não estão em conformidade.

As marcas de pagamento podem definir os programas, mandatos, datas, etc. de conformidade, usando PA-DSS e os aplicativos de pagamento validados listados pelo PCI SSC. Através destes programas de conformidade, as marcas de pagamento promovem o uso dos aplicativos de pagamentos validados da lista.

Conselho dos padrões de segurança da indústria de cartões de pagamento (PCI SSC)

O PCI SSC é o corpo padronizador que mantém os padrões da indústria de cartões de pagamento, incluindo o PCI DSS e o PA-DSS. Em relação com o PA-DSS, o PCI SSC:

- É o repositório centralizado dos Relatórios de validação PA-DSS (ROVs)
- Realize as revisões de Garantia de qualidade (QA) dos ROVs PA-DSS para confirmar a consistência e a qualidade do relatório
- Lista os aplicativos de pagamento validados PA-DSS no site
- Qualifica e treina os PA-QSAs para realizar revisões PA-DSS

- Mantém e atualiza o padrão e a documentação relacionada do PA-DSS de acordo com um processo de gerenciamento de ciclo de vida padrão

Observe que o PCI SSC não aprova os relatórios de uma perspectiva de validação. A função do PA-QSA é documentar a conformidade do aplicativo de pagamento com o PA-DSS a partir da data da avaliação. Além disso, o PCI SSC realiza o QA para garantir que os PA-QSAs documentem as avaliações PA-DSS com precisão e totalmente.

Fornecedores de software

Os fornecedores do software ("fornecedores") desenvolvem aplicativos de pagamento que armazenam, processam ou transmitir dados do proprietário do cartão como parte da autorização ou do estabelecimento e, em seguida, vender, distribuir ou licenciar esses aplicativos de pagamento a terceiros (cliente ou revendedores/integradores). Os fornecedores são responsáveis:

- Pela criação de aplicativos de pagamento em conformidade com o PA-DSS que facilitem e não evitem que seus clientes estejam em conformidade com o PCI DSS (o aplicativo não necessita de implementações ou configurações que viole os requisitos do PCI DSS)
- Por seguir os requisitos sempre que o fornecedor armazenar, processar ou transmitir dados do proprietário do cartão (por exemplo, durante a solução de problemas do cliente)
- Pela criação do *Guia de Implementação PA-DSS*, específico para cada aplicativo de pagamento, de acordo com os requisitos deste documento
- Pela orientação dos clientes, revendedores e integradores sobre como instalar e configurar os aplicativos de pagamento de uma maneira compatível com o PCI DSS
- Por garantir que os aplicativos de pagamento estejam em conformidade com o PA-DSS ao garantir que passem com sucesso na revisão PA-DSS, conforme especificado neste documento

PA-QSAs

Os PA-QSAs são os QSAs que foram qualificados e treinados pelo PCI SSC para realizar as revisões PA-DSS.

Os PA-QSAs são responsáveis:

- Pela realização de avaliações em aplicativos de pagamento de acordo com os Procedimentos de avaliação de segurança e com os Requisitos de validação PA-QSA
- Pelo fornecimento de uma opinião a respeito da conformidade do aplicativo de pagamento com os requisitos do PA-DSS
- Pelo fornecimento de documentação adequada no ROV para demonstrar que o aplicativo de pagamento está em conformidade com o PA-DSS
- Pelo envio do ROV para o PCI SSC, juntamente com o Atestado de validação (assinado pelo PA-QSA e pelo fornecedor)
- Pela manutenção de um processo de garantia de qualidade interno para alcançar o PA-QSA

> ***Observação:*** *Nem todos os QSAs são PA-QSAs - há requisitos adicionais de qualificação que devem ser atendidos para que o QSA passe a ser um PA-QSA.*

É responsabilidade do PA-QSA declarar se o aplicativo de pagamento alcançou a conformidade. O PCI SSC não aprova os ROVs de uma perspectiva de conformidade técnica, mas realiza revisões de QA nos ROVs para garantir que os relatórios documentem adequadamente a demonstração de conformidade.

Revendedores e integradores

Os revendedores e integradores são as entidades que vendem, instalam e/ou prestam serviço de aplicativos de pagamento em nome dos fornecedores do software ou outros. Os revendedores e integradores são responsáveis:

- Pela Implementação de um aplicativo de pagamento em conformidade com o PA-DSS em um ambiente em conformidade com o PCI DSS (ou por instruir o comerciante a fazê-lo)
- Pela configuração do aplicativo de pagamento (onde são fornecidas as opções de configuração), de acordo com o *Guia de Implementação PA-DSS* do fornecedor
- Pela configuração do aplicativo de pagamento (ou por instruir o comerciante a fazê-lo) de um modo compatível com o PCI DSS
- Fornecer serviço de aplicativos de pagamento (por exemplo: solução de problemas, entrega de atualizações remotas e fornecimento de suporte remoto), de acordo com o *Guia de Implementação PA-DSS* e o PCI DSS

Os revendedores e integradores não enviam os aplicativos de pagamento para avaliação. Os produtos apenas são enviados pelo fornecedor.

Clientes

Os clientes são comerciantes, fornecedores de serviço ou outros que compram ou recebem um aplicativo de pagamento de terceiros para armazenar, processar ou transmitir dados do proprietário do cartão como parte da autorização ou estabelecimento das transações de pagamento. Os cliente que quiserem usar os aplicativo que estão em conformidade com o PA-DSS são responsáveis:

> ***Observação:** Apenas um aplicativo de pagamento em conformidade com o PA-DSS não garante que esteja em conformidade com o PCI DSS.*

- Pela Implementação de um aplicativo de pagamento em conformidade com o PA-DSS em um ambiente em conformidade com o PCI DSS
- Pela configuração do aplicativo de pagamento (onde são fornecidas as opções de configuração), de acordo com o *Guia de Implementação PA-DSS* do fornecedor
- Pela configuração do aplicativo de pagamento de um modo em conformidade com o PCI DSS
- Pela manutenção do status de conformidade com o PCI DSS para o ambiente e para a configuração do aplicativo de pagamento

Guia de Implementação PA-DSS

Os aplicativos de pagamento validados devem ser capazes de ser implementados de um modo em conformidade com o PCI DSS. É necessário que os fornecedores do software forneçam um *Guia de Implementação PA-DSS*, que instruam seus clientes e revendedores/integradores sobre a Implementação segura do produto, que documentem as especificidades de configuração segura mencionadas no documento e que delineiem com clareza as responsabilidades do fornecedor, do revendedor/integrador e do cliente para estar em conformidade com os requisitos do PCI DSS. Ele deve detalhar como o cliente e/ou o revendedor/integrador deve ativar as configurações de segurança na rede do cliente. Por exemplo, o *Guia de Implementação PA-DSS* deve tratar das responsabilidade e dos recursos básicos de segurança de senha PCI DSS mesmo se isso não for controlado pelo aplicativo de pagamento, para que o cliente ou revendedor/integrador entenda como implementar senhas seguras para conformidade com o PCI DSS.

Aplicativos de pagamentos, quando implementados de acordo com o *Guia de Implementação PA-DSS* e quando implementados em um ambiente em conformidade com o PCI DSS devem facilitar e fornecer suporte à conformidade com o PCI DSS do cliente.

Consulte *o apêndice A: Resumo do conteúdo do Guia de Implementação do PA-DSS* para comparação das responsabilidades para Implementação dos controles especificados no *Guia de Implementação PA-DSS*.

Requisitos do Avaliador de segurança qualificado do aplicativo de pagamento (PA-QSA)

Apenas os Avaliadores de segurança qualificados do aplicativo de pagamento (PA-QSAs) empregados pelas empresas Avaliadoras de segurança qualificadas (QSA) têm permissão para realizar avaliações PA-DSS. Consulte a lista de Avaliadores de segurança qualificados em www.pcisecuritystandards.org para obter uma lista das empresas qualificadas para realizar as avaliações PA-DSS.

- O PA-QSA deve utilizar os procedimento de teste documentados neste documento padrão de segurança de dados do aplicativo de pagamento.
- O PA-QSA deve ter acesso a um laboratório onde o processo de validação deve ocorrer.

Laboratório de teste

- Podem haver laboratórios de teste em dois locais: no local do PA-QSA ou no local do fornecedor do software.
- O laboratório de teste deve poder simular o uso do aplicativo de pagamento no mundo real.
- O PA-QSA deve validar a instalação simples do ambiente do laboratório para garantir que o ambiente simule com veracidade uma situação da vida real e que o fornecedor não tenha modificado ou falsificado o ambiente de qualquer maneira.
- Consulte o *Apêndice B: Confirmação da Configuração do laboratório de testes específico para avaliação PA-DSS* neste documento para requisitos detalhados para o laboratório e para os processos relacionados ao laboratório.
- O PA-QSA deve preencher e enviar o *Apêndice B,* preenchido para o laboratório específico usado pelo aplicativo de pagamento sob revisão, como parte do relatório PA-DSS completo.

Informações de aplicabilidade PCI DSS

(Retirada do PCI DSS)

O *Padrão de segurança de dados da indústria de cartões de pagamento* (PCI DSS) aplica-se sempre que os dados da conta são armazenados, processados ou transmitidos. *Os dados da conta* são formados por*Dados do proprietário do cartão* mais *Dados de autenticação sensível,* conforme segue.

Os dados do proprietário do cartão incluem:	***Os dados de autenticação sensível incluem:***
▪ O número primário da conta (PAN) ▪ Nome do proprietário de dados ▪ Data de expiração ▪ Código de serviço	▪ Dados da faixa magnética totais ou equivalente em um chip ▪ CAV2/CVC2/CVV2/CID ▪ PINs/Bloqueios de PIN

O número da conta primária (PAN) é um fator decisivo na aplicabilidade dos requisitos PCI DSS e do PA-DSS. Os requisitos do PCI DSS são aplicáveis se o número da conta primária (PAN) for armazenado, processado ou transmitido. Se o PAN não for armazenado, processado ou transmitido, o PCI DSS e o PA -DSS não se aplica.

Se o nome do proprietário do cartão, o código do serviço e/ou a data de expiração forem armazenadas, processadas ou transmitidas com o PAN ou estiverem de qualquer outra forma presentes no ambiente dos dados do proprietário do cartão, eles devem estar protegidos de acordo com todos os requisitos do PCI DSS ***exceto*** os Requisitos 3.3 e 3.4, que aplicam-se apenas ao PAN.

O PCI DSS representa um conjunto mínimo de objetivos de controle que podem ser alcançados por leis e regulamentos locais, regionais ou de setor. Além disso, os requisitos de legislação ou regulatórios podem solicitar proteção específica de informações identificáveis pessoalmente ou outros elementos de dados (por exemplo, nome do proprietário do cartão) ou definir as práticas de divulgação relacionadas às informações do cliente da entidade. Os exemplos incluem legislação relacionada à proteção de dados do consumidor, privacidade, roubo de identidade ou segurança de dados. O PCI DSS não substitui leis locais ou regionais, regulamentos do governo ou outros requisitos legais.

A tabela a seguir do *Padrão de segurança de dados da indústria de cartões de pagamento* (PCI DSS) ilustra elementos comumente utilizados de dados do proprietário do cartão e dados de autenticação sensível, se o **armazenamento** desses dados for permitido ou proibido e se os dados precisam ser **protegidos**. Esta tabela não tem a intenção de ser completa, mas é apresentada para ilustrar o tipo diferente de requisito que aplica-se a cada elemento de dados;

		Elemento de dados	Armazenamento permitido	Processar dados da conta armazenados ilegíveis pelo Requisito 3.4 do PCI DSS
Dados da conta	Dados do proprietário do cartão	O número primário da conta (PAN)	Sim	Sim
		Nome do proprietário de dados	Sim	Não
		Código de serviço	Sim	Não
		Data de expiração	Sim	Não
	Dados de autenticação sensível [1]	Dados da faixa magnética totais [2]	Não	Não é possível armazenar pelo Requisito 3.2
		CAV2/CVC2/CVV2/CID	Não	Não é possível armazenar pelo Requisito 3.2
		PINs/Bloqueio de PIN	Não	Não é possível armazenar pelo Requisito 3.2

Os Requisitos 3.3 e 3.4 do PCI DSS aplicam-se apenas ao PAN. Se o PAN for armazenado com outros elementos dos dados do proprietário do cartão, apenas o PAN deve ser processado como ilegível de acordo com o Requisito 3.4 do PCI DSS.

O PCI DSS ***aplica-se apenas*** se os PANs forem armazenados, processados e/ou transmitidos.

[1] *Os dados de autenticação sensível não devem ser armazenados após a autorização (mesmo se estiverem criptografados).*

[2] *Os dados de rastreamento totais da faixa magnética, dados equivalentes do chip ou em qualquer outro lugar.*

Instruções e conteúdo do relatório de validação

Este documento deve ser usado para os PA-QSAs como modelo para criar o Relatório de Validação. Todos os PA-QSAs devem seguir as instruções deste documento a respeito do conteúdo e formato do relatório ao concluir um relatório de validação.

O Relatório de validação deve conter as seguintes informações como prefácio para os Procedimentos de avaliação de segurança e requisitos:

1. Descrição do escopo de revisão

- Descrever o escopo da cobertura da revisão, pelo escopo da seção PA-DSS acima
- Intervalo de tempo de validação
- Versão do PA-DSS usada para a avaliação
- Lista da documentação revisada

2. Resumo executivo

Inclui o seguinte:

- Nome do produto
- Versão do produto e plataforma relacionada cobertas
- Lista de revendedores e/ou integradores deste produto
- O(s) sistema(s) operacional(is) com os quais o aplicativo de pagamento foi testado
- Software de banco de dados usado ou suportado pelo aplicativo de pagamento
- Descrição breve do aplicativo de pagamento/família de produtos (2-3 frases)
- Diagrama de rede de uma Implementação típica do aplicativo de pagamento (não necessariamente uma Implementação específica do site do cliente) que inclui, em alto nível:
  - Conexões dentro e fora da rede do cliente
  - Componentes da rede do cliente, incluindo dispositivos POS, sistemas, bancos de dados e servidores web conforme aplicável
  - Outro aplicativo de pagamento/componente necessário, conforme aplicável
- Descrição ou diagrama de cada parte do link de comunicação, incluindo (1) LAN, WAN ou Internet, (2) hospedagem da comunicação do software e (3) no host onde o software é implantado (por exemplo, como dois processos diferentes comunicam-se entre si no mesmo host)
- Um diagrama de fluxo de dados que mostra todos os fluxos dos dados do proprietário do cartão, incluindo os fluxos de autorização, captura, ajuste e de cobrança retroativa, conforme aplicável

- Descrição breve dos arquivos e tabelas que armazenam os dados do proprietário do cartão, suportado por um inventário criado (ou obtido do fornecedor do software) e pertencente ao PA-QSA nos papeis de trabalho - este inventário deve incluir, para cada armazenamento de dados do proprietário do cartão (arquivo, tabela, etc.):
  - Lista de todos os elementos dos dados do proprietário do cartão armazenados
  - Como o armazenamento de dados é mantido em segurança
  - Como o acesso ao armazenamento de dados é registrado
- Liste todos os aplicativos de pagamento relacionado aos componentes do software, incluindo requisitos de software de terceiros e dependências
- Descrição dos métodos de autenticação de ponta a ponta do aplicativo, incluindo o mecanismo de autenticação do aplicativo, o banco de dados de autenticação e a segurança do armazenamento de dados
- Descrição da função do aplicativo de pagamento em uma Implementação típica e de quais outros tipos de aplicativos de pagamento são necessários para uma Implementação de pagamento completa
- Descrição do cliente típico para quem este produto é vendido (por exemplo, pequenos, grandes, específicos para um ramo, Internet ou lojas físicas) e a base do cliente do fornecer (por exemplo, segmento de mercado, nomes de grandes clientes).
- Definição da metodologia de versão do fornecedor, para descrever/ilustrar como o fornecedor indica alterações de versão maiores ou menores através dos número de versão e para definir quais tipo de alterações o fornecedor inclui nas alterações de versão maiores ou menores.

> ***Observação:*** Apêndice B: A confirmação da Configuração de laboratório de testes específica para avaliação PA-DSS *também deve ser concluída e enviada com o relatório PA-DSS concluído.*

3. Descobertas e observações

- Todos os PA-QSAs devem usar o modelo a seguir para fornecer descrições e descobertas de relatório detalhadas
- Descreve os testes realizados além daqueles incluídos na coluna de procedimentos de teste.
- Se o avaliador determina que o requerimento não é aplicável para um determinado aplicativo de pagamento, deve-se incluir uma explicação na coluna "Em funcionamento" do requisito.

4. Informações de contato e data do relatório

- Informações de contato do fornecedor de software (inclui URL, número de telefone e endereço de e-mail)
- Informações de contato do PA-QSA (inclui nome, número de telefone e endereço de e-mail)
- Informações de contato primárias de Garantia de qualidade (QA) do PA-QSA (inclui nome do contato de QA primário, número de telefone e endereço de e-mail)
- Data do relatório

Etapas de conclusão PA-DSS

Este documento contém a tabela de Procedimentos de avaliação de segurança e requisitos, assim como no *Apêndice B: Confirmação da Configuração de laboratório de testes específico para avaliação PA-DSS*. Os Procedimentos de avaliação de segurança e requisitos detalham os procedimento que devem ser realizados pelo PA-QSA. O *Apêndice B: A confirmação da Configuração de laboratório de testes específica para avaliação PA-DSS* deve ser concluída pelo PA-QSA para confirmar o status e as capacidades do laboratório de testes usado para conduzir esta avaliação.

O PA-QSA deve realizar as seguintes etapas:

1. Conclua o relatório de validação usando este documento como modelo:
   a. Conclua o prefácio do relatório de validação, de acordo com a seção intitulada "Instruções e conteúdo dos relatórios de validação"
   b. Conclua e documente todas as etapas detalhadas nos Procedimentos de avaliação de segurança e requisitos, incluindo descrições breves dos controles observados na coluna "Em funcionamento" e anotando comentários. *Observe que o relatório com qualquer opinião "Em funcionamento" não deve ser enviado para o PCI SSC até que todos os itens sejam anotados como "Em funcionamento".*
2. Apêndice B completo *: Confirmação da Configuração de laboratório de testes específico para avaliação PA-DSS.*
3. Conclua e assine *um Atestado de validação* (PA-QSA e fornecedor do software). O Atestado de validação está disponível no site do PCI SSC (www.pcisecuritystandards.org).
4. Após a conclusão, envie todos os documentos acima para o PCI SSC de acordo com o *Guia do programa PA-DSS.*

Guia do programa PA-DSS

Consulte o *Guia do programa PA-DSS* para obter informações sobre o gerenciamento de programa PA-DSS , incluindo os tópicos:

- Processos de aceitação e envio de relatório PA-DSS
- Processo de renovação anual para aplicativos de pagamento incluídos na lista de aplicativos PA-DSS validados
- Transição de aplicativos validados para PABP para a lista de aplicativos de pagamento PA-DSS validados
- As responsabilidades de notificação do evento um aplicativo de pagamento listado é determinado para ser falha no compromisso.

O PCI SSC reserva-se o direito de requisitar a revalidação devido a mudanças significativas no Padrão de segurança de dados de aplicativo de pagamento e/ou devido a vulnerabilidades especificamente identificadas em um aplicativo de pagamento listado.

Requisitos e procedimentos de avaliação de segurança PA-DSS

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
1. Não possui faixa magnética total, código de verificação de cartão ou valor (CAV2, CID, CVC2, CVV2) ou dados de bloqueio de PIN				
1.1 Não armazene dados de autenticação sensível após a autorização (mesmo se estiverem criptografados): Os dados de autenticação sensível incluem os dados, conforme citado nos Requisitos 1.1.1 até 1.1.3. ***Observações****:* ▪ *Ao proibir o armazenamento dos dados de autenticação sensível após a autorização, assume-se que a transação tenha concluído o processo de autorização e que o cliente tenha recebido a aprovação da transação final. Após a conclusão da autorização, estes dados de autenticação sensível não podem ser armazenados.* ▪ *É permissível para os emissores e empresas que suportam os serviços de emissão para armazenar dados de autenticação sensível se houver justificação de negócios e se os dados forem armazenados com segurança.* ***Alinha-se com o Requisito 3.2 PCI DSS***	**1.1.a** Se este aplicativo de pagamento armazena dados de autenticação sensível, verifique se o aplicativo foi desenvolvido apenas para emissores e/ou empresas que suportam serviços de emissão.			
	1.1.b Para todos os outros aplicativos de pagamento, se os dados de autenticação sensível (consulte 1.1.1-1.1.3, abaixo) tiverem sido armazenados anteriormente à autorização e depois excluídos, obtiver e revisar a metodologia para excluir os dados para determinar que os dados sejam irrecuperáveis.			
	1.1.c Para cada item dos dados de autenticação sensível abaixo, realize as etapas a seguir após concluir diversas transações de teste que simulam todas as funções do aplicativo de pagamento, para incluir geração de condições de erro e de entradas de log.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
1.1.1 Após a autorização, não armazene todo o conteúdo de qualquer rastreamento da faixa magnética (localizada na parte de trás do cartão, dados equivalentes contidos no chip ou em qualquer outro lugar). Esses dados são alternativamente chamados de rastreamento total, rastreamento, rastreamento 1, rastreamento 2 e dados de faixa magnética. ***Observação:*** *No curso normal dos negócios, os seguintes elementos de dados da faixa magnética podem necessitar de retenção:* ▪ *O nome do titular da conta,* ▪ *O número da conta primária (PAN),* ▪ *Data de expiração e* ▪ *Código de serviço* *Para minimizar os riscos, armazene apenas os elementos de dados necessários para os negócios.* ***Alinha-se com o Requisito 3.2.1 do PCI DSS***	**1.1.1** Use as ferramentas e/ou métodos (ferramentas comercial, scripts, etc.)[3] a examina todas as saídas criadas pelo aplicativo de pagamento e verifica se todos os conteúdos de qualquer rastreamento da faixa magnética da parte de trás do cartão ou dados equivalentes no chip não estão armazenados após a autorização. Inclui pelo menos os seguintes tipos de arquivos (assim como qualquer outra entrada gerada pelo aplicativo de pagamento): ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastreamento ▪ Memória não-volátil, incluindo cache não volátil ▪ Esquemas de banco de dados ▪ Conteúdos do banco de dados			

[3] Ferramenta ou método forense: Ferramenta ou método para descoberta, análise e apresentação de dados forenses, que fornece uma maneira robusta de autenticar, buscar e recuperar evidências do computador rápida e totalmente. No caso de ferramentas ou métodos forenses usados pelos PA-QSAs, essas ferramentas ou método devem localizar com precisão quaisquer dados de autenticação sensível gravados pelo aplicativo de pagamento. Essas ferramentas podem ser comerciais, de fonte aberta ou desenvolvidas internamente pelo PA-QSA.

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
1.1.2 Após a autorização, não armazene o valor de verificação ou o código do cartão (número de três ou quatro dígitos impresso na parte frontal ou de trás do cartão de pagamento) usado para verificar transações em que o cartão não estava presente. ***Alinha-se com o Requisito 3.2.2 do PCI DSS***	**1.1.2** Use as ferramentas e/ou métodos (ferramentas comercial, scripts, etc.) para examinar todas as saídas criadas pelo aplicativo de pagamento e verifique se o código de verificação de três ou quatro dígitos impresso na frente do cartão ou no painel de assinaturas (dados CVV2, CVC2, CID, CAV2) não estejam armazenados após a autorização. Inclui pelo menos os seguintes tipos de arquivos (assim como qualquer outra entrada gerada pelo aplicativo de pagamento): ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastreamento ▪ Memória não-volátil, incluindo cache não volátil ▪ Esquemas de banco de dados ▪ Conteúdos do banco de dados			
1.1.3 Após a autorização, não armazene o número de identificação pessoal (PIN) ou o bloqueio de PIN criptografado. ***Alinha-se com o Requisito 3.2.3 do PCI DSS***	**1.1.3** Use as ferramentas e/ou métodos (ferramentas comercial, scripts, etc.) para examinar todas as saídas criadas pelo aplicativo de pagamento e verifique se os PINs e os bloqueios de PIN criptografados não são armazenados após a autorização. Inclui pelo menos os seguintes tipos de arquivos (assim como qualquer outra entrada gerada pelo aplicativo de pagamento). ▪ Dados de transação de entrada ▪ Todos os registros (por exemplo, transação, histórico, depuração, erro) ▪ Arquivos do histórico ▪ Arquivos de rastreamento ▪ Memória não-volátil, incluindo cache não volátil ▪ Esquemas de banco de dados ▪ Conteúdos do banco de dados			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
1.1.4 Exclua com segurança dados da faixa magnética, valores ou códigos de verificação do cartão e PINs ou dados de bloqueio de PIN armazenados por versões anterior do aplicativo de pagamento, de acordo com padrões aceitos pela indústria para exclusão segura, como definido, por exemplo, pela lista de produtos aprovados mantidos pela Agência de segurança nacional ou por outros padrões ou regulamentos estaduais ou nacionais. ***Observação:*** *Os requisitos aplicam-se apenas se as versões anteriores do aplicativo de pagamento armazenaram dados de autenticação sensível.* ***Alinha-se com o Requisito 3.2 do PCI DSS***	**1.1.4.a** Revise o *Guia de Implementação PA-DSS* preparado pelo fornecedor e verifique se a documentação inclui as instruções a seguir para os clientes e revendedores/integradores: ▪ Esses dados históricos devem ser removidos (dados da faixa magnética, código de verificação do cartão, PINs ou bloqueios de PIN armazenados por versões anteriores do aplicativo de pagamento) ▪ Como remover dados do histórico ▪ Essa remoção é absolutamente necessária para conformidade PCI DSS			
	1.1.4.b Verifique se o fornecedor fornece uma ferramenta ou procedimento de limpeza seguros para remover os dados.			
	1.1.4.c Verifique, através do uso de ferramentas e/ou métodos forenses, se a ferramenta ou procedimento de limpeza segura fornecida pelo fornecedor remove os dados com segurança , de acordo com os padrões aceitos pela indústria para a exclusão segura de dados.			
1.1.5 Exclua com segurança dados de autenticação sensível (dados pré-autorização) usados para fins de depuração ou solução de problemas dos arquivos de registros, arquivos de depuração e outras fontes de dados recebidas dos cliente, para garantir que os dados da faixa magnética, os códigos e valores de verificação do cartão e os dados de PIN e de bloqueio de PIN não estejam armazenados nos sistema do fornecedor do software. Essas fontes de dados devem ser coletadas em quantias limitadas e apenas quando necessárias para resolver um problema, criptografadas enquanto armazenadas e excluídas imediatamente após o uso. ***Alinha-se com o Requisito do 3.2 PCI DSS***	**1.1.5.a** Examine os procedimentos do fornecedor do software para solução de problemas do cliente e verifique se os procedimentos incluem: ▪ Coleta de dados de autenticação confidenciais somente quando necessário para solucionar problemas específicos. ▪ Armazenamento de tais dados em locais específicos e conhecidos, com acesso limitado. ▪ Coleta somente de uma quantidade de dados limitada para solucionar algum problema específico. ▪ Criptografia de dados de autenticação confidenciais enquanto estiverem armazenados. ▪ Exclusão segura de tais dados, imediatamente após o uso			
	1.1.5.b Selecione uma amostra de solicitações de resolução de problemas recentes e verificar cada evento seguido do procedimento examinado no item 1.1.5.a.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
	1.1.5.c Revise o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verificação se a documentação inclui as seguintes instruções para clientes e revendedores/integradores: ▪ Coletar de autenticação confidencial somente quando necessário para solucionar problemas específicos. ▪ Armazenar tais dados somente em locais específicos e conhecidos, com acesso limitado. ▪ Coletar somente de uma quantidade limitada de dados para solucionar algum problema específico. ▪ Criptografar dados de autenticação confidenciais enquanto estiverem armazenados. ▪ Excluir com segurança de tais dados imediatamente após o uso.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2. Proteger os dados armazenados do titular do cartão				
2.1 O fornecedor do software deve oferecer orientações a clientes sobre o expurgo de dados do portador do cartão após o vencimento do período de retenção definido pelo cliente. ***Alinha-se com o Requisito 3.1 do PCI DSS***	**2.1** Revise o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verificação se a documentação inclui as seguintes orientações para clientes e revendedores/integradores: ▪ Exclusão dos dados do portador do cartão que excedem o período de retenção definido pelo cliente. ▪ Uma lista com todos os locais onde o aplicativo de pagamento armazena dados do portador do cartão (para que o cliente saiba os locais dos dados que precisam ser excluídos). ▪ Instruções para configurar os softwares ou sistemas subjacentes (como SO, bancos de dados, etc.) para evitar captura ou retenção inadvertidas de dados do portador do cartão. Por exemplo, o sistema faz backup ou recupera pontos.			
2.2 Mascare o PAN quando exibido (os primeiros seis e quatro últimos dígitos são o número máximo de dígitos a serem exibidos). ***Observações:*** ▪ *Esse requisito não se aplica aos funcionários e outras partes interessadas em um negócio legítimo que precisam visualizar o PAN completo.* ▪ *Este requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do portador do cartão - por exemplo, para recebimentos do ponto de venda.* ***Alinha-se com o Requisito 3.3 do PCI DSS***	**2.2** Revise as exibições de dados do cartão de crédito, incluindo sem limitações os dispositivos de pontos de venda, telas, logs e recibos, para determinar se os números de cartões de crédito são mascarados ao exibir os dados do portador do cartão, exceto para aqueles com uma necessidade empresarial específica de visualizar todos os números do cartão de crédito.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2.3 Converta o PAN como ilegível em qualquer local onde ele esteja armazenado (inclusive em em mídia digital portátil, mídia de back-up, em registros), utilizando qualquer uma das seguintes abordagens: ▪ Referências únicas com base na criptografia robusta (o hash deve ser de todo o PAN) ▪ Truncamento (a codificação hash não pode ser usada para substituir o segmento truncado do PAN) ▪ Tokens e blocos de índice (os blocos devem ser armazenados de forma segura) ▪ Criptografia robusta com processos e procedimentos de gerenciamento-chave associados. ***Observações:*** ▪ *É um esforço relativamente pequeno para que um indivíduo malicioso reconstrua os dados do PAN original caso ele tenha acesso tanto à versão truncada quanto à hash de um PAN. Onde as versões hash e truncada de um mesmo PAN forem geradas por um aplicativo de pagamento, controles adicionais devem estar posicionados para assegurar que as versões truncada e hash não possam estar correlacionadas para reconstruir o PAN original.* ▪ *O PAN deve ser convertido como ilegível em qualquer local que é armazenado, mesmo fora do aplicativo de pagamento.* ***Alinha-se com o Requisito 3.4 do PCI DSS***	**2.3** Verifique se o PAN for convertido como ilegível em qualquer local em que foi armazenado, de acordo com o seguinte.			
	2.3.a Examine o método usado para proteger o PAN, inclusive os algoritmos de criptografia (se aplicável). Verifique se o PAN for tornado ilegível usando um dos seguintes métodos: ▪ Referências únicas com base na criptografia robusta. ▪ Truncamento ▪ Tokens e blocos de índice, sendo que os blocos são armazenados de forma segura ▪ Criptografia robusta, com processos e procedimentos de gerenciamento-chave associados			
	2.3.b Examine muitas tabelas ou arquivos dos repositórios de dados criados ou gerados pelo aplicativo para verificar se o PAN foi tornado ilegível.			
	2.3.c Se o aplicativo criar ou gerar arquivos para o uso em outros aplicativos (por exemplo, arquivos gerados para exportação ou backup), inclusive para armazenamento em mídias removíveis, examine uma amostra de de arquivos gerados, inclusive aqueles gerados em mídias removíveis (por exemplo fitas de beakup), para confirmar que o PAN foi convertido ilegível.			
	2.3.d Examine uma amostra de logs de auditoria criados ou gerados pelo aplicativo para confirmar que o PAN foi convertido ilegível ou removido dos logs.			
	2.3.e Se o fornecedor do software armazenar o PAN por qualquer motivo (por exemplo, porque arquivos de log, arquivos de depuração e outras origens de dados são recebidas de clientes para fins de depuração e resolução de problemas), verifique se o PAN é convertido como ilegível de acordo com os Requisitos 2.3.a até o 2.3.d do PCI DSS acima.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2.4 Se a criptografia de disco for utilizada (em vez da criptografia de bancos de dados no nível de arquivo ou coluna), o acesso lógico deve ser gerenciamento independentemente de mecanismos de controle de acesso a sistemas operacionais nativos (por exemplo, não utilizando bancos de dados de contas de usuário locais). As chaves da descrição não devem estar ligadas às contas de usuário**.** ***Alinha-se com o Requisito 3.4.2 do PCI DSS***	**2.4** Se a criptografia de disco for usada, verifique se foi implementada da seguinte maneira:			
	2.4.a Verifique se o acesso lógico aos sistemas de arquivos criptografados foi implementado por meio de um mecanismo que seja separado do mecanismo de sistemas operacionais nativos (por exemplo, não usando os bancos de dados das contas de usuário locais).			
	2.4.b Verifique se as chaves criptográficas são armazenadas de forma segura (por exemplo, armazenadas nas mídias removíveis que estão protegidas adequadamente com controles de acesso robustos).			
	2.4.c Se o aplicativo criar ou gerar arquivos em mídias removíveis, verifique se os dados do portador do cartão nas mídias removíveis estão cripografadas em qualquer lugar que estejam,			
2.5 O aplicativo de pagamento deve proteger as chaves de criptografia utilizadas para criptografia de dados do portador do cartão em relação a divulgações ou mau uso. ***Observação:*** *Este requisito também se aplica às principais chaves de criptografia usadas para proteger chaves de criptografia de dados—tais chaves de criptografia de chaves devem ser ao menos tão robustas quanto a chave de criptografia de dados.* ***Alinha-se com o Requisito 3.5 do PCI DSS***	**2.5** Verifique se aplicativo de pagamento deve proteger as chaves de criptografia utilizadas para criptografia de dados do portador do cartão em relação a divulgações ou mau uso, da seguinte maneira:			
	2.5.a Analise a metodologia usada pelo aplicativo para proteger as chaves, para verificar se os controles foram implementados para restringir o acesso às chaves.			
	2.5.b Analise os arquivos de configuração do sistema para verificar se as chaves estão armazenadas no formato criptografado e se as chaves de criptografia de chaves estão armazenadas separadamente das chaves de criptografia de dados.			
	2.5.c Analise o *Guia de Implementação PA-DSS* preparado pelo fornecedor e verifique se os clientes e os revendedores e integradores sejam aconselhados a: ▪ Restringir o acesso às chaves ao menor número necessário de responsáveis pela proteção. ▪ Armazenar chaves de forma segura no menor número possível de locais e formatos.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2.6 O aplicativo de pagamento deve implementar processos e procedimentos de gerenciamento de chaves criptográficas para as chaves utilizadas para criptografia de dados do portador do cartão. ***Alinha-se com o Requisito 3.6 do PCI DSS***	**2.7.a** Revise o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verificação se a documentação inclui as seguintes instruções para clientes e revendedores/integradores: ▪ Como gerar, distribuir, proteger, alterar, armazenar e inutilizar/substituir chaves de criptografia, onde os clientes ou revendedores/integradores estiverem envolvidos nessas atividades de gerenciamento de chaves. ▪ Uma amostra de formulário para que os responsáveis por chaves confirmem que compreendem e aceitam suas responsabilidades como responsável por chave. ▪ Como realizar funções de gerenciamento de chaves definidas no 2.6.1 até o 2.6.7 abaixo, conforme exigido para conformidade com o PCI DSS.			
	2.6.b Verifique se o aplicativo de pagamento implementa técnicas de gerenciamento de chaves, conforme o Requisito 3.6 do PCI DSS.			
2.6.1 Geração de chaves criptográficas robustas	**2.6.1** Verifique se os procedimentos de gerenciamento-chave foram implementados para exigir a geração de chaves robustas.			
2.6.2 Distribuição segura de chaves criptográficas	**2.6.2** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir a distribuição segura de chaves.			
2.6.3 Armazenamento seguro de chaves criptográficas	**2.6.3** Verifique se os procedimentos do gerenciamento-chave foram implementados para exigir o armazenamento seguro de chaves.			
2.6.4 Alterações em chaves criptográficas para chaves que alcançaram o final de seu criptoperíodo (por exemplo, após um período de tempo definido ter passado e/ou após certa quantidade de texto-cifrado ter sido produzido por determinada chave), conforme definido pelo fornecedor associado do aplicativo ou pelo proprietário da chave e baseado nas melhores práticas e orientações da indústria (por exemplo, a NIST Special Publication 800-57).	**2.6.4** Verifique se os procedimentos de gerenciamento de chave foram implementados para reforçar as alterações de chave ao final do criptoperíodo.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2.6.5 Inutilização ou substituição de chaves (por exemplo: por arquivamento, destruição e ou revogação conforme for aplicável)conforme for considerado necessário quando a integridade da chave estiver enfraquecida (por exemplo, a saída de um funcionário com conhecimento de uma chave em texto simples, etc.) ou chaves estiverem supostamente comprometidas. ***Observação:*** *Caso chaves criptográficas inutilizadas ou recolocadas precisarem ser retidas, essas chaves deverão ser arquivadas em segurança (por exemplo, usando uma chave de criptografia de chaves). Chaves criptográficas arquivadas deveriam ser usadas somente para fins de decodificação/verificação.*	**2.6.5.a**Verifique se os procedimentos de gerenciamento de chaves foram implementados para inutilizar chaves quando a integridade da chave tiver sido enfraquecida.			
	2.6.5.b Verifique se os procedimentos do gerenciamento de chaves foram implementados para substituir chaves suposta ou sabidamente comprometidas.			
	2.6.5.c Caso chaves criptográficas sejam retidas, verifique qual alicativo não usa essas chaves para operações de codificação.			
2.6.6 Se o aplicativo do pagamento suportar operações de gerenciamento manual em texto simples de chaves criptográficas, essas operações deverão reforçar o conhecimento partilhado e o controle duplo (por exemplo, a exigência para que duas ou três pessoas, cada uma conhecendo somente sua parte da chave). ***Observação:*** *Exemplo de operações de gerenciamento manual de chaves incluem não se limitam a: geração da chave, transmissão, carregamento, armazenamento e destruição.*	**2.6.6** Verifique se o manual sobre os procedimentos de gerenciamento de chaves em texto simples.			
2.6.7 Prevenção contra a substituição não autorizada de chaves criptográficas	2.6.7 Verifique se os procedimentos do gerenciamento de chaves foram implementados para exigir a prevenção contra a substituição não autorizada das chaves.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
2.7 Converta o material da chave irrecuperável ou qualquer material criptografado armazenado por versões anteriores do aplicativo de pagamento, de acordo com os padrões aceitos pelo setor. Essas são as chaves criptográficas utilizadas para criptografar ou verificar os dados do portador do cartão. ***Observações:*** ▪ *Materiais de chaves criptográficas e/ou criptogramas podem ser convertidos para irrecuperáveis através do uso de ferramentas de processamento inclusive, mas não se limitando a:* – *Exclusão segura, conforme definida, por exemplo, na lista de produtos aprovados mantidos pela National Security Agency (Agência Nacional de Segurança) ou por outras regulamentações ou padrões nacionais ou estaduais.* – *A exclusão da chave de criptografia de chave (KEK) desde que chaves de criptografia de dados residuais estejam criptografadas pela KEK excluída.* ▪ *Esse requisito aplica-se somente se versões anteriores do aplicativo de pagamento utilizaram materiais de chave criptográfica ou criptogramas para criptografar dados do portador do cartão.* ***Alinha-se com o Requisito 3.6 do PCI DSS***	**2.7.a** Revise o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verificação se a documentação inclui as seguintes instruções para clientes e revendedores/integradores: ▪ Esse material criptografado deve ser convertido para irrecuperável. ▪ Como criptografar o para irrecuperável. ▪ Essa característica de irrevogável é absolutamente necessária para conformidade PCI DSS ▪ Como criptografar novamente dados do histórico com novas chaves			
	2.7.b Verificar se o fornecedor oferece uma ferramenta de limpeza ou procedimento para converter o material criptográfico para irrecuperável.			
	2.7.c Verificar, por meio do uso de ferramentas e/ou métodos forenses, se a ferramenta de limpeza segura ou procedimento converte o material criptográfico em irrecuperável, de acordo com os padrões aceitos pelo setor.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcion amento	Fora de funcion amento	Data de destino/ Comentários
3. Fornecer recursos de autenticação segura				
3.1 O aplicativo de pagamento deve suportar e reforçar o uso de IDs de usuário exclusivos e assegurar a autenticação para todo acesso administrativo e para todo acesso aos dados de um portador de cartão. A autenticação segura deve ser reforçada para todas as contas, geradas ou gerenciadas pelo aplicativo, pela conclusão da instalação e pelas alterações subsequentes após a instalação. O aplicativo deve exigir o seguinte: ***Observação:*** *Esses controles de senha não se destinam a aplicar-se a equipes que somente possuem acesso a um número de cartão no momento para facilitar uma única transação. Esses controles são aplicáveis para o acesso pelo pessoal com capacidades administrativas, para acesso a sistemas com dados do portador do cartão e para acesso controlado pelo aplicativo de pagamento.* *Esse requisito destina-se ao aplicativo de pagamento e todas as ferramentas associadas para visualizar ou acessar os dados do portador do cartão.* ***Alinha-se com os Requisitos de PCI DSS 8.1, 8.2, e 8.5.8–8.5.15***	**3.1.c** *Examine o Guia de Implementação do PA-DSS* criado para verificar o seguinte: ▪ Os clientes e revendedores/integradores são informados que o aplicativo de pagamento reforça a autenticação segura para todas as credenciais que o aplicativo gera ao: – Reforçar as alterações seguras nas credenciais de autenticação no momento da conclusão da instalação (Consulte abaixo do 3.1.1 até o 3.1.10). – Reforçar alterações seguras para as que forem subsequentes (após a instalação) para as credenciais de autenticação (Consulte abaixo do 3.1.1 até o 3.1.10) ▪ Clientes e revendedores/integradores devem atribuir autenticação segura a quaisquer contas padrão (mesmo se não forem utilizadas) e então desativar ou não utilizar essas contas. ▪ Quando credenciais de autenticação são usadas pelo aplicativo de pagamento (mas não são geradas ou gerenciadas pelo aplicativo), clientes e revendedores recebem direções claras e precisas sobre como, ao concluir a instalação e para quaisquer alterações após a instalação, alterar as credenciais de autenticação e criar uma autenticação forte pelos Requisitos 3.1.1 até 3.1.10 abaixo, para todas as contas do nível do aplicativo com acesso administrativo e para todos os acessos aos dados do portador do cartão.			
	3.1.b Testar o aplicativo de pagamento para verificar se o aplicativo não utiliza (ou requer o uso de) contas administrativas padrão para outros softwares necessários (por exemplo, o aplicativo de pagamento não deve usar a conta administrativa para software de banco de dados).			
	3.1.c Caso o aplicativo de pagamento gere ou gerencie credenciais de autenticação, teste o aplicativo para verificar se ele reforça alterações a quaisquer senhas padrão do aplicativo de pagamento ao concluir o proceso de instalação.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
	3.1.d Para contas que são geradas ou gerenciadas pelo aplicativo, teste o aplicativo para verificar se ele reforça IDs de usuário exclusivos e autenticação segura de acordo com o 3.1.1 até 3.1.10 abaixo, para todo acesso administrativo e todo acesso aos dados de portadores do cartão. Assegure-se que os requisitos de autenticação segura sejam reforçados: – Ao concluir o processo de instalação e – Para alterações subsequentes após a instalação. (Exemplos de alterações subsequentes incluem mas não se limitam a quaisquer alterações que resultem na reversão de contas de usuários para definições padrão, quaisquer alterações em definições de contas existentes e alterações que gerem novas contas ou recriem contas existentes.)			
3.1.1 O aplicativo de pagamento atribui IDs únicas para contas de usuários. ***Alinha-se com o Requisito 8.1 do PCI DSS***	**3.1.1** Confirme que o aplicativo de pagamento atribui IDs únicas para contas de usuários.			
	3.1.1.a Ao concluir o processo de instalação.			
	3.1.1.b Para alterações subsequentes após a instalação.			
3.1.2O aplicativo de pagamento emprega ao menos um dos seguintes métodos para autenticar todos os usuários: ▪ Algo que você conheça, como uma senha ou frase de confirmação ▪ Algo que você tenha, como um dispositivo de token ou um smart card ▪ Algo que você é, como a biométrica ***Alinha-se com o Requisito 8.2 do PCI DSS***	**3.1.2**Confirme se o aplicativo de pagamento exige ao menos um dos métodos de autenticação definidos:			
	3.1.2.a Ao concluir o processo de instalação.			
	3.1.2.b Para alterações subsequentes após a instalação.			
3.1.3 O aplicativo de pagamento **não** exige ou usa nenhuma conta de grupo, compartilhada ou genérica e nem senhas.	**3.1.3** Confirme que o aplicativo de pagamento não usa nem depende de nenhuma conta de grupo, compartilhada ou genérica e nem senhas:			
	3.1.1.a Ao concluir o processo de instalação			

Requisitos do PA-DSS	Procedimentos de teste	Em funcion amento	Fora de funcion amento	Data de destino/ Comentários
Alinha-se com o Requisito 8.5.8 do PCI DSS				
	3.1.3.b Para alterações subsequentes após a instalação.			
3.1.4O aplicativo de pagamento exige alterações à senha do usuário no mínimo a cada 90 dias. ***Alinha-se com o Requisito 8.5.9 do PCI DSS***	**3.1.4** Confirme se o aplicativo de pagamento exige que os usuários alterem suas senhas no mínimo a cada 90 dias:			
	3.1.4.a Ao concluir o processo de instalação			
	3.1.4.b Para alterações subsequentes após a instalação.			
3.1.5 O aplicativo de pagamento exige um tamanho mínimo de senha se pelo menos sete caracteres. ***Alinha-se com o Requisito 8.5.10 do PCI DSS***	**3.1.5** Confirme se o pagamento exige que as senhas tenham pelo menos sete caracteres de tamanho:			
	3.1.5.a Ao concluir o processo de instalação			
	3.1.5.b Para alterações subsequentes após a instalação.			
3.1.6 O aplicativo de pagamento exige que senhas contenham tanto caracteres numéricos quanto alfabéticos. ***Alinha-se com o Requisito 8.5.11 do PCI DSS***	**3.1.6** Confirme que o aplicativo de pagamento exige que as senhas contenham tanto caracteres numéricos quanto alfabéticos.			
	3.1.6.a Ao concluir o processo de instalação			
	3.1.6.b Para alterações subsequentes após a instalação.			
3.1.7 O aplicativo de pagamento mantém o histórico de senhas e exige que uma nova senha seja diferente das últimas quatro senhas usadas. ***Alinha-se com o Requisito 8.5.12 do PCI DSS***	**3.1.7** Confirme se o aplicativo de pagamento mantém o histórico de senhas e exige que uma nova senha seja diferente das últimas quatro senhas usadas.			
	3.1.7.a Ao concluir o processo de instalação			
	3.1.7.b Para alterações subsequentes após a instalação.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcion amento	Fora de funcion amento	Data de destino/ Comentários
3.1.8 O aplicativo de pagamento limita as tentativas repetidas de acesso ao bloquear a conta de usuário depois de não mais do que seis tentativas de logon. ***Alinha-se com o Requisito 8.5.13 do PCI DSS***	**3.1.8** Confirme que o pagamento bloqueia a conta de usuário depois de não mais do que seis tentativas de logon inválidas.			
	3.1.8.a Ao concluir o processo de instalação			
	3.1.8.b Para alterações subsequentes após a instalação.			
3.1.9 O aplicativo de pagamento define a duração do bloqueio para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário. ***Alinha-se com o Requisito 8.5.14 do PCI DSS***	**3.1.9** Confirme se o aplicativo de pagamento bloqueia as contas de usuário por um mínimo de 30 minutos ou até um administrador do sistema reiniciar a conta.			
	3.1.9.a Ao concluir o processo de instalação			
	3.1.9.b Para alterações subsequentes após a instalação.			
3.1.10 Se uma sessão do aplicativo de pagamento estiver ociosa por mais do que 15 minutos, o aplicativo exigira que o usuário autentique e ative a sessão novamente. ***Alinha-se com o Requisito 8.5.15 do PCI DSS***	**3.1.10** Confirme se o pagamento define o tempo limite de ociosidade de uma sessão para 15 minutos ou menos.			
	3.1.10.a Ao concluir o processo de instalação			
	3.1.10.b Para alterações subsequentes após a instalação.			
3.2 O fornecedor do software deve oferecer orientação aos clientes de que todo acesso a PCs, servidores e bancos de dados com aplicativos de pagamento devem exigir um ID de usuário exclusivo e uma autenticação segura. ***Alinha-se com o Requisito 8.1 e 8.2 do PCI DSS***	**3.2** Examine o *Guia de Implementação do PA-DSS* criado pelo fornecedor para verificar se os clientes e revendedores/integradores foram recomendados a controlar o acesso, por meio de um ID de usuário exclusivo e uma autenticação segura compatível com o PCI DSS, a qualquer PC, servidor e bancos de dados com os aplicativos de pagamento e os dados do portador do cartão.			
3.3 Deixa as senhas do aplicativo de pagamento ilegíveis durante a transmissão e o armazenamento, usando criptografia robusta baseada nos padrões aprovados. ***Alinha-se com o Requisito 8.4 do PCI DSS***	**3.3** Examine os arquivos de senha do aplicativo de pagamento durante o armazenamento e a transmissão para verificar se as senhas estão ilegíveis em todos os momentos.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
4. Registrar em log a atividade do aplicativo de pagamento				
4.1 Após a conclusão do processo de instalação, a instalação padrão pronta para uso do aplicativo de pagamento deve registrar em log todos os acessos de usuários (especialmente usuários com privilégios administrativos) e deve poder ligar todas as atividades a usuários individuais. ***Alinha-se com o Requisito 10.1 do PCI DSS***	**4.1.a** Examine as configurações do aplicativo de pagamento para verificar se as trilhas de auditoria do aplicativo de pagamento são ativadas automaticamente ou ficam disponíveis para ativação pelos clientes.			
	4.1.b Se as configurações de log do aplicativo de pagamento puderem ser configuradas pelo cliente e revendedores/integradores, ou os clientes ou revendedores/integradores são responsáveis pela Implementação do log, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor para verificar se as seguintes informações foram incluídas: ▪ Como definir as configurações de log em conformidade com o PCI DSS, de acordo com os Requisitos 4.2 e 4.4 do PA-DSS abaixo. ▪ Os logs não devem ser desabilitados e, caso isso ocorra, resultará em inconformidade com o PCI DSS.			
4.2 O aplicativo de pagamento deve fornecer uma trilha de auditoria para reconstruir os seguintes eventos: ***Alinha-se com o Requisito 10.2 do PCI DSS***	**4.2** Teste o aplicativo de pagamento e examine os logs de auditoria e suas definições, então realize o seguinte:			
4.2.1 Todos os acessos individuais aos dados do portador do cartão a partir do aplicativo	**4.2.1** Verifique se todos os acessos individuais aos dados do portador do cartão por meio do aplicativo de pagamento estão registrados.			
4.2.2 Todas as ações tomadas por qualquer indivíduo com privilégios administrativos conforme atribuídas no aplicativo	**4.2.2** Verifique se todas as ações tomadas por qualquer indivíduo com privilégios administrativos no aplicativo de pagamento estão registradas			
4.2.3 Acesso às trilhas de auditoria gerenciadas pelo ou no aplicativo	**4.2.3** Verifique se o acesso às trilhas de auditoria gerenciadas pelo ou no aplicativo está registrado.			
4.2.4 Tentativas inválidas de acesso lógico	**4.2.4** Verifique se as tentativas inválidas de acesso lógico estão registradas.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
4.2.5 Uso dos mecanismos de identificação e autenticação do aplicativo	**4.2.5**Verifique se o uso dos mecanismos de identificação e autenticação do aplicativo está registrado.			
4.2.6 Inicialização dos registros de auditoria do aplicativo	**4.2.6**Verifique se a inicialização dos registros de auditoria está registrada.			
4.2.7 Criação e exclusão de objetos no nível do sistema no ou pelo aplicativo	**4.2.7** Verifique se a criação e exclusão de objetos no nível do sistema no ou pelo aplicativo estão registradas			
4.3 O aplicativo de pagamento deve registrar no mínimo as seguintes entradas de trilhas de auditoria para cada evento: ***Alinha-se com o Requisito 10.3 do PCI DSS***	**4.3** Teste o aplicativo de pagamento e examine os logs de auditoria e suas definições, então, para cada evento auditável (desde o 4.2), realize o seguinte:			
4.3.1 Identificação do usuário	**4.3.1**Verifique se a identificação do usuário está incluída nas entradas do registro.			
4.3.2 Tipo de evento	**4.3.2**Verifique se o tipo de evento está incluído nas entradas do registro.			
4.3.3 Data e horário	**4.3.3**Verifique se a data e o horário estão incluídos nas entradas do registro.			
4.3.4 Indicação de sucesso ou falha	**4.3.4**Verifique se a indicação de êxito ou falha está incluída nas entradas do registro.			
4.3.5 Origem do evento	**4.3.5**Verifique se a origem do evento está incluída nas entradas do registro.			
4.3.6A identidade ou o nome dos dados afetados, componentes do sistema ou recurso	**4.3.6**Verifique se a identidade ou o nome dos dados afetados, componentes do sistema ou recursos estão incluídos nas entradas do registro.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
4.4. O aplicativo de pagamento deve facilitar o registro centralizado. ***Observação:*** *Os exemplos dessa funcionalidade podem incluir, mas não são limitados a:* ▪ Registro por meio de mecanismos padrão de arquivos de log do setor tais como o Sistema Comum de Arquivos de Log (CLFS), Syslog, texto delimitado, etc. ▪ Fornecimento de funcionalidade e documentação para converter o formato de log próprio do aplicativo em formatos padrão do setor, adequados para logs centralizados, de notificação. ***Alinha-se com o Requisito 10.5.3 do PCI DSS***	**4.4.a** Valide que o aplicativo de pagamento forneça funcionalidade que facilite a habilidade de um comerciante assimilar logs em seu servidor de logs centralizado.			
	4.4.b Examine o *Guia de Implementação PA-DSS* preparado pelo fornecedor para verificar se clientes e revendedores/integradores tenham recebido instruções e procedimentos para a incorporação dos logs do aplicativo de pagamento em um ambiente centralizado de log.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
5. Desenvolver aplicativos de pagamento seguros				
5.1 O fornecedor de software desenvolve aplicativos de pagamento de acordo com o PCI DSS e o PA-DSS (por exemplo, autenticação segura e registros) e com base nas melhores práticas do setor, além de incorporar a segurança das informações em todo o ciclo de vida do desenvolvimento dos softwares. Esses processos devem incluir o seguinte: ***Alinha-se com o Requisito 6.3 do PCI DSS***	**5.1.a** Obtenha e axemine os processos de desenvolvimento de software por escrito para verificar se os processos são baseados nos padrões e/ou nas melhores práticas do setor .			
	5.1.b Verifique se a segurança da informação está inclusa através do ciclo de vida de desenvolvimento do software.			
	5.1.c Verifique se os aplicativos do software são desenvolvidos de acordo com os Requisitos do PCI DSS e do PA-DSS.			
	5.1.d A partir da examinação de processos de desenvolvimento de software por escrito, entrevistas com desenvolvdores de software e examinação do produto final do aplicativo de pagamento, verifique se:			
5.1.1 PANs reais não são utilizados para testes ou desenvolvimento. ***Alinha-se com o Requisito 6.4.3 do PCI DSS***	**5.1.1** PANs reais não são utilizados para testes ou desenvolvimento.			
5.1.2 Remoção de dados e contas de teste antes da entrega ao cliente. ***Alinha-se com o Requisito 6.4.4 do PCI DSS***	**5.1.** 5.1.2 Remoção de dados e contas de teste antes da entrega ao cliente.			
5.1.3 Remoção de contas, IDs de usuário e senhas personalizadas do aplicativo de pagamento antes que seja liberado aos clientes ***Alinha-se com o Requisito 6.3.1 do PCI DSS***	**5.1.3** Contas, IDs de usuário e senhas personalizadas do aplicativo de pagamento são removidas antes que seja liberado aos clientes.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
5.1.4 Revisão do código do aplicativo de pagamento antes da liberação aos clientes após qualquer alteração significativa, para identificar qualquer possível vulnerabilidade na codificação. ***Observação:*** *Esse requisito referente às análises dos códigos se aplica a todos os componentes do aplicativo de pagamento (internos e voltados para o público), como parte integrante do ciclo de vida de desenvolvimento do sistema. As análises dos códigos podem ser realizadas por equipes internas instruídas ou terceiros.* ***Alinha-se com o Requisito 6.3.2 do PCI DSS***	**5.1.4** Confirma que o fornecedor executa revisões de código para todas as alterações significativas de código do aplicativo (usando processos manuais ou automatizados), conforme se segue: ▪ As alterações dos códigos são analisadas por outras pessoas além do autor que originou o código e por pessoas que estão cientes das técnicas de análise dos códigos e das práticas de codificação seguras. ▪ As revisões de código garantem que o código seja desenvolvido segundo diretrizes de codificação seguras. (Consulte o Requisito do 5.2 PA-DSS.) ▪ As correções adequadas são implementadas antes da liberação. ▪ Os resultados das análises dos códigos são revisados e aprovados pela gerência antes da liberação.			
5.2 Desenvolver todos os aplicativos de pagamento (internos e externos e inclusive acesso administrativo ao produto pela web) com base nas orientações de codificação seguras. Cobrir a prevenção de vulnerabilidades de codificação comuns nos processos de desenvolvimento do software, para incluir: ***Observação:*** *As vulnerabilidades listadas nos Requisitos 5.2.1 a 5.2.9 do PA-DSS e 6.5.1 a 6.5.9 do PCI DSS estavam atualizadas com as melhores práticas do setor quando* esta versão do *PADSS foi lançada. No entanto, como as melhores práticas do setor para o gerenciamento da vulnerabilidade foram atualizadas (por exemplo, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), as melhores práticas atuais devem ser usadas para esses requisitos.* ***Alinha-se com o Requisito 6.5 do PCI DSS***	**5.2.a** Obtenha e revise os processos de desenvolvimento de software para qualquer aplicativo de pagamento (interno e externo, inclusive acesso administrativo na web ao produto). Verifique se o processo inclui treinamento em técnicas de codificação segura para desenvolvedores, com base nas melhores práticas e orientações do setor.			
	5.2.b Entreviste alguns desenvolvedores e obtenha uma comprovação de que eles estão instruídos sobre as técnicas de codificação seguras.			
	5.2.c Verifique se os aplicativos de pagamento não estão sujeitos a vulnerabilidades de codificação comuns por meio da realização de testes de penetração manuais ou automáticos que especificamente tentam explorar cada um dos seguintes itens:			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
5.2.1 Falhas na injeção, particularmente na injeção SQL. Também considere as falhas de injeção de OS Command Injection, LDAP e Xpath, assim como outras falhas.	**5.2.1** Falhas na injeção, particularmente na injeção SQL (validar a entrada para verificar se os dados do usuário não podem modificar o significado dos comandos e das consultas).			
5.2.2 Buffer Overflow	**5.2.2** Buffer Overflow (Valide os limites do buffer e trunque as strings de entrada)			
5.2.3 Armazenamento criptográfico seguro	**5.2.3** Armazenamento criptográfico inseguro (Impeça a ocorrência de falhas criptográficas.)			
5.2.4 Comunicações inseguras	**5.2.4** Comunicações inseguras (Criptografe de forma adequada todas as comunicações autenticadas e confidenciais.)			
5.2.5 Manuseio incorreto de erros	**5.2.5** Manuseio incorreto de erros (não deixe vazar informações por meio de mensagens de erro e outras formas)			
5.2.6 Todas as vulnerabilidades "altas" conforme identificadas no processo de identificação de vulnerabilidade no Requisito 7.1 do PA-DSS	**5.2.6** Todas as vulnerabilidades "altas" conforme identificadas no processo de identificação de vulnerabilidade no Requisito 7.1 do PA-DSS			
Observação: *Os requerimentos 5.2.7 a 5.2.9 abaixo, são válidos para aplicativos e interfaces de aplicativos baseados em rede (interna ou externa):*				
5.2.7 Scripting de site cruzado (XSS)	**5.2.7** Scripting de site cruzado (XSS) (Valide todos os parâmetros antes da inclusão, utilize a saída sensível ao contexto, etc.).			
5.2.8 Controle incorreto de acesso como referências inseguras diretas a objetos, falha ao restringir acesso a URLs e diretório transversal	**5.2.8** Referências inseguras diretas a objetos (Autentique os usuários e transforme a entrada adequadamente. Não exponha referências de objetos internos aos usuários.)			
5.2.9 Falsificação de solicitações de site cruzado (CSRF)	**5.2.5** Falsificação de solicitações de site cruzado (CSRF) (não responda as credenciais e tokens de autorização enviados automaticamente pelos navegadores.)			
5.3 O fornecedor do software deve seguir os procedimentos de controle de alteração para todas as alterações de configuração do software. Os procedimentos devem incluir o seguinte: ***Alinha-se com o Requisito 6.4.5 do PCI DSS***	**5.3.a** Obtenha e examine os procedimentos de controle de alterações para modificações no software e verificar se os procedimentos exigem os requisitos 5.3.1–5.3.4, a seguir.			
	5.3.b Examinar alterações recentes no aplicativo de pagamento e rastrear essas alterações com a documentação de controle de alteração relacionada. Verificar se, para cada alteração examinada, o seguinte foi documentado de acordo com os procedimentos de controle de alteração:			

Requisitos do PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
5.3.1 Documentação de impacto	**5.3.1** Verifique se a documentação do impacto no cliente está incluída na documentação de controle de alteração para cada alteração.			
5.3.2 Aprovação documentada da alteração por partes autorizadas	**5.3.2** Verifique se a aprovação documentada da alteração por partes autorizadas está presente em todas as alterações.			
5.3.3 Teste de funcionalidade para verificar se a alteração não tem impacto adverso sobre a segurança do sistema.	**5.3.3.a** Para toda amostra de alteração, verifique se o teste de funcionalidade foi realizado para verificar se a alteração não tem impacto adverso sobre a segurança do sistema			
	5.3.3.b Verifique se todas as alterações (inclusive de patches) foram testadas quanto a conformidade com o 5.2 antes de serem lançadas.			
5.3.4 Procedimentos de desistência ou desinstalação do produto	**5.3.4** Verifique se os procedimentos de desistência ou desinstalação do produto estão preparados para cada alteração.			
5.4 O aplicativo de pagamento deve utilizar ou requisitar o uso de serviços, protocolos, daemons, componentes assim como softwares e hardwares dependentes necessários e seguros, inclusive os fornecidos por terceiros, para qualquer funcionalidade do aplicativo de pagamento (por exemplo, caso NetBIOS, compartilhamento de arquivos, Telnet, FTP, etc. sejam requisitados pelo aplicativo, serão segurados pela SSH, a S-FTP, SSL, IPSec ou outra tecnologia). ***Alinha-se com o Requisito 2.2.2 do PCI DSS***	**5.4.a Examine** os serviços, protocolos, daemons, componentes, assim como softwares e hardwares dependentes do sistema ativados ou exigidos pelo aplicativo do sistema. Verifique se somente os serviços, protocolos, daemons, componentes, assim como softwares e hardwares dependentes do sistema necessários estão ativados como prontos para o uso por padrão			
	5.4.b Caso o aplicativo suporte quaisquer serviços, protocolos, daemons ou comonentes inseguros, verifique se eles estão configurados por padrão como prontos para o uso.			
	5.4.c Verifique se o *Guia de Implementação do PA-DSS* documenta todos os protocolos, serviços, componentes, bem como softwares e hardwares dependentes que sõ necessários para qualquer funcionalidade do aplicativo de pagamento, inclusive aquelas oferecidas por terceiros.			
6. Proteger transmissões wireless				
6.1 Para aplicativos de pagamento que utilizem a tecnologia wireless, altere o padrão de wireless do fornecedor, inclusive, mas não limitado a suas chaves de criptografia, senhas e strings de comunidade de SNMP. A tecnologia wireless	**6.1** Para aplicativos de pagamento desenvolvidos pelo fornecedor utilizando tecnologia wireless, e outros aplicativos wireless em conjunto com o aplicativo de pagamento, verifique se os aplicativos wireless não utilizam as configurações padrão do fornecedor, como a seguir:			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
deve ser implementada com segurança. ***Alinha-se com o Requisito 1.2.3 e 2.1.1 do PCI DSS***	**6.1.a** Verifique se as chaves de criptografia foram alteradas do padrão na instalação e são modificadas a qualquer momento que um funcionário que conheça as chaves sai da empresa ou troca de cargo			
	6.1.b Verifique se as strings de comunidades de SNMP padrão nos dispositivos sem fio foram alteradas			
	6.1.c Verifique se as senhas/passphrases padrão nos pontos de acesso foram alteradas			
	6.1.d Verifique se o firmware nos dispositivos sem fio foi atualizado para ser compatível com a criptografia robusta para a autenticação e a transmissão em redes sem fio			
	6.1.e Verifique outros padrões do fornecedor sem fio relacionados à segurança, se aplicável			
	6.1.f Examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor para verificar se os clientes e revendedores/integradores estão instruídos, se a comunicação sem fio for utilizada, para: ▪ Alterar os padrões de wireless do fornecedor conforme definido em 6.1.a - 6.1 ou mais; ▪ Instalar um firewall entre quaisquer redes e sistemas wireless que armazenem dados de portadores de cartão e ▪ Configurar esses firewalls para recusar ou controlar (se esse tráfego for necessário para fins comerciais) qualquer tráfego a partir do ambiente sem fio no ambiente de dados do portador do cartão.			
6.2 Para aplicativos de pagamento usando tecnologia wireless, o aplicativo de pagamento deve facilitar o uso das melhores práticas do setor (por exemplo, IEEE 802.11i) para implementar uma criptografia robusta para autenticação e transmissão.	**6.2.a** Para aplicativos de pagamento desenvolvidos pelo fornecedor usando tecnologia wireless, e para outros aplicativos wireless fornecidos com o aplicativo do fornecedor, verifique se as melhores práticas do setor (por exemplo, IEEE 802.11.i) foram usadas para incluir ou para disponibilizar criptografia robusta para autenticação e transmissão.			

Requisitos do PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
Observação: *O uso de WEP como controle de segurança foi proibido em 30 de junho de 2010.* ***Alinha-se com o Requisito 4.1.1 do PCI DSS***	**6.2.b** Se os clientes puderem armazenar dados do portador do cartão em um servidor conectado à Internet, examine o Guia de Implementação do PA-DSS preparado pelo fornecedor para verificar se os clientes e revendedores/integradores são instruídos sobre as configurações wireless compatíveis com o PCI DSS, inclusive sore a alteração de padrões do fornecedor (em 6.1.a - p-1 ou mais) e sobre o uso das melhores práticas do setor para implementar uma criptografia robusta para a autenticação e transmissão de dados do portador do cartão. (em 6.2.a).			

Requisitos PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
7. Testar aplicativos de pagamento para solucionar vulnerabilidades				
7.1 Os fornecedores de software devem estabelecer um processo para identificar e atribuir um ranqueamento de risco às vulnerabilidades na segurança descobertas recentemente além de testar seus aplicativos de pagamento quanto a vulnerabilidades. Qualquer software ou sistema subjacente fornecido ou exigido pelo aplicativo de pagamento (por exemplo, servidores, bibliotecas ou programas de terceiros) devem ser incluídos nesse processo. ***Alinha-se com o Requisito 6.2 do PCI DSS*** ***Observação:*** *Rankings de risco devem ser baseados nas melhores práticas do setor. Por exemplo, os critérios para ranquear vulnerabilidades como "Alta" risco deve incluir uma pontuação base no CVSS de 4,0 ou mais e/ou um patch oferecido pelo fornecedor que este classifique como "crucial" e/ou uma vulnerabilidade que afete um componente crucial do aplicativo.*	**7.1** Obter e examinar os processos para identificar novas vulnerabilidades e para testar os aplicativos de pagamento para novas vulnerabilidades. Esses processos devem incluir o seguinte:			
	7.1.a Verifique se os processos incluem atribuir um ranking de risco a vulnerabilidades. (No mínimo, as mais cruciais, as maiores vulnerabilidades devem ser ranqueadas com o "Alta".)			
	7.1.b Verifique se o processo para identificar novas vulnerabilidades no sistema incluem o uso de fontes externas para informações sobre a vulnerabilidade da segurança			
	7.1.c Verifique se os processos incluem o teste dos aplicativos de pagamento para novas vulnerabilidades			
	7.1.b Verificar se os processos para identificar novas vulnerabilidades e implementar correções no aplicativo de pagamento aplicam-se a todos os softwares fornecidos ou exigidos pelo aplicativo de pagamento (por exemplo, servidores web, bibliotecas e programas de terceiros).			
7.2 Os fornecedores de software devem estabelecer um processo para o desenvolvimento e implantação oportunos de patches e upgrades de segurança, que incluem ofertas de atualizações e patches de forma segura com uma cadeira de confiança conhecida e manutenção da integridade do código de patch e atualização durante a oferta e a implantação.	**7.2.a** Obter e examinar os processos para desenvolver e implantar patches de segurança e upgrades para software. Verifique se os processos incluem a Implementação pontual e a Implementação de patches para os clientes			
	7.2.b Revise os procesos para verificar se os patches e atualizações foram fornecidos de forma segura com uma uma conhecida corrente-de-conhecimento			
	7.2.c Revise os processos para verificar se os patches e atualizações de modo a manter a integridade dessas ofertas			
	7.2.d Revise os processos para verificar se os patches e atualizações foram testados quanto a sua integridade no sistema de destino antes da instalação			

Requisitos PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
	7.2.b Para verificar que a integridade do patch e do código de atualização é mantida, execute o processo de atualização dom código arbitrário e determine se o sistema não permite que a atualização ocorra.			
8. Facilitar a Implementação de rede segura				
8.1 O aplicativo de pagamento deve poder ser implementado em um ambiente de rede seguro. O aplicativo não deve interferir com o uso de dispositivos, aplicativos ou configurações exigidos para conformidade com o PCI DSS (por exemplo, o aplicativo de pagamento não pode interferir com a proteção antivírus, configurações de firewall ou qualquer outro dispositivo, aplicativo ou configuração exigidos para conformidade com o PCI DSS). ***Alinha-se com o Requisito 8.1 e 8.2 do PCI DSS***	**8.1** Teste o aplicativo de pagamento em um laboratório para obter evidências de que pode ser executado em uma rede totalmente compatível com o PCI DSS. Verificar se o aplicativo de pagamento não inibe a instalação de patches ou atualizações em outros componentes no ambiente.			
9. Os dados do portador do cartão nunca devem ser armazenados em servidores conectados à Internet				
9.1 O aplicativo de pagamento deve ser desenvolvido de modo que o servidor do banco de dados e o servidor web não precisem estar no mesmo servidor, nem o servidor do banco de dados precise estar no DMZ com o servidor web. ***Alinha-se com o Requisito 1.3.7 do PCI DSS***	**9.1.a** Para verificar se o aplicativo de pagamento armazena os dados do portador do cartão na rede interna, e nunca no DMZ, obtenha evidências de que o aplicativo de pagamento não exija armazenamento de dados no DMZ, e permita o uso de um DMZ para separar a Internet de sistemas que armazenam dados do portador do cartão (por exemplo, o aplicativo de pagamento não deve exigir que o servidor do banco de dados e o servidor web estejam no mesmo servidor ou no DMZ com o servidor web).			
	9.1.b Se os clientes puderem armazenar dados do portador do cartão em um servidor conectado à Internet, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor para verificar se os clientes e revendedores/integradores sabem que não podem armazenar os dados do portador do cartão em sistemas acessíveis para Internet (por exemplo, o servidor web e o servidor do banco de dados não devem estar no mesmo servidor).			

Requisitos PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
10. Facilitar o acesso remoto seguro ao aplicativo de pagamento				
10.1 O aplicativo de pagamento não deve interferir no uso de tecnologias de autenticação de dois fatores para acesso remoto seguro. (Por exemplo, RADIUS com tokens, TACACS com tokens ou outras tecnologias que facilitam a autenticação de dois fatores.) ***Observação:*** *A autenticação de dois fatores exige que dois dos três métodos de autenticação (veja abaixo) sejam usados para a autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não caracteriza autenticação de dois fatores. Os métodos de autenticação, também conhecidos como métodos, são:* ▪ *Algo que você conheça, como uma senha ou frase de confirmação* ▪ *Algo que você tenha, como um dispositivo de token ou um smart card* ▪ *Algo que você é, como a biométrica* ***Alinha-se com o Requisito 8.3 PCI DSS***	**10.1** Teste o aplicativo de pagamento em um laboratório para obter a evidência de que ele não interfere nas tecnologias de autenticação de dois fatores.			
10.2 Se o aplicativo de pagamento puder ser acessado remotamente, o acesso remoto ao aplicativo de pagamento deve ser autenticado usando um mecanismo de autenticação de dois fatores. ***Observação:*** *A autenticação de dois fatores exige que dois dos três métodos de autenticação (veja abaixo) sejam usados para a autenticação (consulte o Req. 10.1 do PA-DSS para obter descrições dos métodos de autenticação).* ***Alinha-se com o Requisito 8.3 do PCI DSS***	**10.2** Se o aplicativo de pagamento puder ser acessado remotamente, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor do software e verifique se contém instruções para clientes e revendedores/integradores a respeito do uso de autenticação de dois fatores (dois dos três métodos de autenticação descritos no Req. 10.1 do PA DSS).			

Requisitos PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
10.3 Qualquer acesso remoto ao aplicativo de pagamento deve ser feito em segurança, conforme se segue:	**10.3** Verifique se todo acesso remoto é feito do seguinte modo:			
10.3.1 Se as atualizações do aplicativo de pagamento forem entregues por meio de acesso remoto nos sistemas dos clientes, os fornecedores de software devem avisar os clientes para ativar as tecnologias de acesso remoto somente quando necessário para efetuar downloads do fornecedor e desativar imediatamente após sua conclusão. De forma alternativa, se entregue via VPN ou outra conexão de alta velocidade, os fornecedores de software devem avisar os clientes para configurar corretamente um firewall ou produto de firewall pessoal para proteger as conexões sempre ativas. ***Alinha-se com o Requisito 1 e 12.3.9 do PCI DSS***	**10.3.1** Se o fornecedor entregar o aplicativo de pagamento e/ou atualizações por meio de acesso remoto às redes do cliente, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verifique se nele contém: ▪ Instruções para clientes e revendedores/integradores a cerca do uso seguro de tecnologias de acesso remoto, especificando que as tecnologias de acesso remoto usadas por fornecedores e parceiros comerciais devem ser ativadas somente quando necessário e desativadas imediatamente após o uso. ▪ Recomendações para clientes e revendedores/integradores a utilizar um firewall configurado com segurança ou produto de firewall pessoal se o computador estiver conectado via VPN ou outra conexão de alta velocidade para proteger conexões sempre ativas, de acordo com o Requisito 1 do PCI DSS.			

<table>
<tr><th>Requisitos PA-DSS</th><th>Procedimentos de teste</th><th>Em funcionamento</th><th>Fora de funcionamento</th><th>Data de destino/ Comentários</th></tr>
<tr><td rowspan="2">10.3.2 Se fornecedores, revendedores/integradores ou clientes puderem acessar remotamente os aplicativos de pagamento do cliente, o acesso remoto deve ser implementado de forma segura.

Observação: Exemplos de recursos de segurança de acesso remoto incluem:
▪ Alteração das configurações padrão no software de acesso remoto (por exemplo, alteração de senhas padrão e uso de senhas exclusivas para cada cliente).
▪ Permitir conexões somente de endereço IP/MAC específicos (conhecidos).
▪ Usar autenticação robusta e senhas complexas para logins (Consulte os Requisitos 3.1.1 a 3.1.10 do PA-DSS)
▪ Ativar a transmissão de dados criptografados de acordo com o Requisito 12.1 do PCI DSS.
▪ Ativar o bloqueio de conta após um determinado número de tentativas de login sem sucesso (Consulte o Requisito 3.1.8 do PA-DSS)
▪ Configuração do sistema de modo que um usuário remoto estabeleça uma conexão de rede virtual privada (“VPN”) por meio de um firewall antes que o acesso seja permitido.
▪ Ativação da função de registro em log.
▪ Restrição do acesso a senhas do cliente à equipe do revendedor/integrador autorizada.
▪ Estabelecimento de senhas de cliente de acordo com os Requisitos 3.1 a 3.1.10 do PA-DSS.

Alinha-se com o Requisito 8.3 do PCI DSS</td>
<td>10.3.2.a Se o fornecedor do software utilizar produtos de acesso remoto para acesso remoto ao aplicativo do cliente, verifique se a equipe do fornecedor implementa e usa recursos de segurança de acesso remoto.</td><td></td><td></td><td></td></tr>
<tr><td>10.3.2.b Se revendedores/integradores ou clientes puderem usar o software de acesso remoto, examine o Guia de Implementação do PA-DSS preparado pelo fornecedor de software e verifique se os clientes e revendedores/integradores foram orientados a usar e implementar os recursos de segurança de acesso remoto.</td><td></td><td></td><td></td></tr>
</table>

Requisitos PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
11. Criptografar tráfego sensível por redes públicas				
11.1 Se o aplicativo de pagamento enviar ou facilitar o envio de dados do portador do cartão por redes públicas, o aplicativo de pagamento deve apoiar o uso de criptografia potente e protocolos de segurança (por exemplo, SSL/TLS e internet protocol security (IPSEC), SSH, etc.) para para proteger dados confidenciais do portador do cartão durante a transmissão em redes públicas, abertas. *Os exemplos de redes abertas e públicas que estão no escopo do PCI DSS são:* ▪ *A Internet* ▪ *Tecnologias sem fio* ▪ *Global System for Mobile communications (GSM)* ▪ *General Packet Radio Service (GPRS)* ***Alinha-se com o Requisito 4.1 do PCI DSS***	**11.1.a** Se o aplicativo de pagamento enviar ou facilitar o envio de dados do portador do cartão por redes públicas, verifique se são fornecidos cripografia potente e protocolos de segurança ou se seu uso é especificado.			
	11.1.b Se o aplicativo de pagamento permitir a transmissão de dados por rede públicas, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verifique se o fornecedor inclui orientações para que os clientes e revendedores/integradores utilizem tecnologia de transmissão de criptografia segura e protocolos de segurança.			
11.2 Se o aplicativo de pagamento facilitar o envio de PANs por tecnologias de mensagem do usuário final (por exemplo, e-mail, mensagens instantâneas, chat), O aplicativo de pagamento deve oferecer uma solução que converta o PAN ilegível, implemente criptografia potente ou especifique o uso de uma para criptografar os PANs. ***Alinha-se com o Requisito 4.2 do PCI DSS***	**11.2.a** Se o aplicativo de pagamento permitir e/ou facilitar o envio de PANs por tecnologias de envio de mensagens de usuário final, verifique se alguma solução de criptografia robusta é fornecida ou se seu uso é especificado.			
	11.2.b Se o aplicativo de pagamento permitir e/ou facilitar o envio de PANs por tecnologias de sistema de mensagens de usuário final, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verifique se o fornecedor inclui orientações para clientes e revendedores/integradores para utilizar uma solução de que implemente criptografia robusta.			

Requisitos do PA-DSS	Procedimentos de teste	Em funciona mento	Fora de funcion amento	Data de destino/ Comentários
12. Criptografar todos os acessos administrativos não-console				
12.1 Orientar clientes a criptografar todos os acessos administrativos não-console usando tecnologias como SSH, VPN ou SSL/TLS para gerenciamento baseado em web e outros acessos administrativos não-console. ***Observação:*** *Nunca se deve utilizar Telnet ou rlogin para acesso administrativo.* ***Alinha-se com o Requisito 2.3 do PCI DSS***	**12.1** Se o aplicativo de pagamento ou servidor permitir administração não-console, examine o *Guia de Implementação do PA-DSS* preparado pelo fornecedor e verifique se o fornecedor recomenda o uso de SSH, VPN ou SSL/TLS para criptografia de acesso administrativo não-console.			
13. Manter documentação educativa e programas de treinamento para clientes, revendedores e integradores				
13.1 Desenvolver, manter e disseminar o *Guia de Implementação do PA-DSS* para clientes, revendedores e integradores que cumpra o seguinte:	**13.1** Examine o *Guia de Implementação do PA-DSS* e os processos relacionados e verifique se o guia é disseminado a todos os usuários relevantes do aplicativo de pagamento (incluindo clientes, revendedores e integradores).			
13.1.1 Atendem a todos os requisitos contidos neste documento sempre que é feita referência ao *Guia de Implementação do PA-DSS*.	**13.1.1** Verifique se o *Guia de Implementação do PA-DSS* aborda todos os requisitos relacionados neste documento.			
13.1.2 Incluem uma revisão pelo menos anual e fazem atualizações para manter a documentação em dia com todas as alterações de software grandes e pequenas em relação aos requisitos deste documento.	**13.1.2.a** Verifique se o *Guia de Implementação do PA-DSS* é revisado anualmente e atualizado conforme a necessidade para documentar todas as alterações grandes e pequenas no aplicativo de pagamento.			
	13.1.2.b Verifique se o *Guia de Implementação do PA-DSS* é revisado anualmente e atualizado conforme a necessidade para documentar todas as alterações aos requisitos do PA-DSS.			
13.2 Desenvolver e implementar programas de treinamento e comunicação para garantir que os revendedores e integradores do aplicativo de pagamento saibam implementar o aplicativo de pagamento e os sistemas e redes relacionados de acordo com o *Guia de Implementação do PA-DSS* e de forma compatível com o PCI DSS.	**13.2** Examine os materiais de treinamento e o programa de comunicação para revendedores e integradores e confirme se os materiais abordam todos os itens observados relacionados ao *Guia de Implementação do PA-DSS* em todo o documento.			

Requisitos do PA-DSS	Procedimentos de teste	Em funcionamento	Fora de funcionamento	Data de destino/ Comentários
13.2.1 Atualize anualmente os materiais de treinamento e sempre que uma nova versão do aplicativo de pagamento for liberada.	**13.2.1.a** Examine os materiais de treinamento para revendedores e integradores e verifique se os materiais são revisados anualmente e quando novas versões do aplicativo de pagamento forem lançadas e atualizadas conforme a necessidade.			
	13.2.1.b Examine o processo de distribuição para novas versões do aplicativo de pagamento e verifique se a documentação atualizada é distribuída com o aplicativo de pagamento atualizado.			
	13.2.1.b Selecione alguns revendedores e integradores e entreviste-os para verificar se receberam os materiais de treinamento.			

Anexo A: Resumo do conteúdo do *Guia de Implementação do PA-DSS*

O objetivo deste Anexo é resumir os requisitos do PA-DSS que possuem tópicos relacionados ao *Guia de Implementação do PA-DSS,* para explicar o conteúdo do *Guia de Implementação do PA-DSS* e para explicar detalhadamente as responsabilidades pela Implementação dos controles relacionados.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
1.1.4	Exclusão de dados de autenticação confidenciais armazenados por versões anteriores do aplicativo de pagamento.	▪ Os dados históricos devem ser removidos (dados da faixa magnética, código de verificação do cartão, PINs ou bloqueios de PIN armazenados por versões anteriores do aplicativo de pagamento) ▪ Como remover dados do histórico ▪ Tal remoção é absolutamente necessária para a conformidade com o PCI DSS.	**Fornecedor de software**: Fornecer ferramenta ou procedimento para que os clientes removam com segurança os dados armazenados por versões anteriores, de acordo com o Requisito 1.1.4 do PA-DSS. **Clientes e revendedores/Integradores**: Excluir quaisquer dados do histórico conforme o *Guia de Implementação do PA-DSS* e o Requisito 1.1.4 do PA-DSS.
1.1.5	Exclusão de quaisquer dados de autenticação confidenciais (pré-autorização) recolhidos como resultado da resolução de problemas com o aplicativo de pagamento.	▪ Dados de autenticação confidenciais (pré-autorização) somente devem ser coletados quando necessário para resolver problemas específicos ▪ Tais dados devem ser armazenados somente em locais específicos e conhecidos, com acesso limitado. ▪ Coleta somente de uma quantidade limitada de tais dados para solucionar algum problema específico. ▪ Os dados de autenticação confidenciais devem ser criptografados enquanto estiverem armazenados. ▪ Tais dados devem ser excluídos de forma segura imediatamente após o uso.	**Fornecedor de software**: Solucione qualquer problema do cliente de acordo com o Requisito 1.1.5.a do PA-DSS. **Clientes e revendedores/Integradores:** Solucione quaisquer problemas conforme o *Guia de Implementação do PA-DSS* e o Requisito 1.1.6.a do PA-DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
2.1	Eliminação dos dados do portador do cartão após o período de retenção definido pelo cliente.	▪ Os dados do portador do cartão devem ser eliminados assim que excederem o período de retenção definido pelo cliente. ▪ Todos os locais onde o aplicativo de pagamento armazena dados do portador do cartão.	**Fornecedor de software**: Oferecer orientação a clientes informando que os dados do portador do cartão que excedem o período de retenção definido pelo cliente devem ser eliminados e onde tais dados são armazenados pelo aplicativo de pagamento. **Clientes e revendedores/Integradores**: Eliminar os dados do portador do cartão que excedem o período de retenção definido pelo cliente.
2.5	Proteção das chaves de criptografia utilizadas para criptografia de dados do portador do cartão em relação a divulgações ou mau uso.	▪ Restringir o acesso às chaves ao menor número necessário de responsáveis pela proteção. ▪ Armazenar chaves de forma segura no menor número possível de locais e formatos.	**Fornecedor de software**: Orientar os clientes que as chaves usadas para dar segurança aos dados do portador do cartão devem ser armazenadas em segurança no menor número de locais possível e com acesso restrito ao menor número possível de responsáveis. **Clientes e revendedores/Integradores**: Armazenar as chaves em segurança no menor número de locais possível e restringir o acesso ao menor número possível de responsáveis.
2.6	Implementação processos e procedimentos de gerenciamento para chaves criptografadas usadas para a criptografia de dados do portador do cartão.	▪ Como gerar, distribuir, proteger, alterar, armazenar e inutilizar/substituir chaves de criptografia, onde os clientes ou revendedores/integradores estiverem envolvidos nessas atividades de gerenciamento de chaves. ▪ Uma amostra de formulário para que os responsáveis por chaves confirmem que compreendem e aceitam suas responsabilidades como responsável por chave. ▪ Como realizar funções de gerenciamento de chaves definidas no 2.6.1 até o 2.6.7 abaixo.	**Fornecedor de software**: Orientar os clientes que acessam as chaves criptográficas usadas na criptografia dos dados do portador do cartão para implementarem os processos e procedimentos de gerenciamento de chaves. **Clientes e revendedores/Integradores**: Implementar processos e procedimentos de gerenciamento para chaves criptográficas usadas para a criptografia dos dados do portador do cartão segundo o *Guia de Implementação do PA-DSS* e o Requisito 2.6 do PA-DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
2.7	Conversão de material chave criptográfico irrecuperável ou criptogramas armazenados por versões anteriores do aplicativo de pagamento.	▪ O material criptografado deve ser convertido para irrecuperável. ▪ Como criptografar o material criptográfico para irrecuperável. ▪ Essa característica de irrevogável é absolutamente necessária para conformidade PCI ▪ Como criptografar novamente dados do histórico com novas chaves	**Fornecedor de software**: Oferecer ferramenta ou procedimento para remover com segurança o material chave criptográfico ou criptogramas armazenados por versões anteriores, de acordo com o Requisito 1.1.5 do PA-DSS, fornecer ferramenta ou procedimento para criptografar novamente os dados do histórico com novas chaves. **Clientes e revendedores/Integradores**: Excluir quaisquer materiais criptográficos do histórico conforme o *Guia de Implementação do PA-DSS* e o Requisito 1.1.5 do PA-DSS.
3.1	Uso de IDs de usuário exclusivos e autenticação segura para acesso administrativo e acesso a dados do portador do cartão.	▪ O aplicativo de pagamento reforça a autenticação segura para todas as credenciais de autenticação (como usuários, senhas) que o aplicativo gera ao: – Reforçar as alterações seguras nas credenciais de autenticação no momento da conclusão da instalação para qualquer alteração subsequente (após a instalação) conforme os requisitos (Consulte abaixo do 3.1.1 até o 3.1. ▪ Atribuir autenticação segura para todas as contas padrão (mesmo se não utilizadas) e desativar ou não utilizar as contas. ▪ Como alterar e criar credenciais de autenticação quando tais credenciais não são geradas ou gerenciadas pelo aplicativo de pagamento, conforme os Requisitos 8,5 a 8.5.15, no momento da conclusão da instalação e para alterações subsequentes após a instalação, para contas de todos os níveis do aplicativo, com acesso administrativo ou acesso aos dados do portador do cartão.	**Fornecedor de software**: Quando o aplicativo de pagamento gerar ou gerenciar credenciais de autenticação, assegurar que o aplicativo de pagamento reforce o uso do cliente de IDs de usuário exclusivos e tornar segura a autenticação para contas/senhas do aplicativo, conforme os Requerimentos 3.1.1 a 3.1.1 do PA_DSS. Quando as credenciais de autenticação não forem geradas ou gerenciadas pelo aplicativo de pagamento, assegurar que o *Guia de Implementação do PA-DSS* ofereça orientações claras e precisas para clientes e revendedores/integradores sobre como alterar e criar credenciais de autenticação seguras conforme os Requisitos 3.1.1 a 3.1.10 do PA-DSS. **Clientes e revendedores/Integradores**: Estabelecer e manter IDs de usuário exclusivos e autenticação segura de acordo com o *Guia de Implementação do PA-DSS* e os Requisitos 3.1.1 a 3.1.10 do PCI DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
3.2	Uso de IDs de usuário exclusivos e autenticação segura para acesso a PCs, servidores e bancos de dados com aplicativos de pagamento.	Uso de nomes de usuário exclusivos e autenticação segura para acesso a qualquer PC, servidor e bancos de dados com aplicativos de pagamento e/ou dados do portador do cartão, de acordo com os Requisitos 3.1.1 a 3.1.10 do PA-DSS.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para uso de IDs de usuário exclusivos e autenticação segura para contas/senhas se definido pelo fornecedor para acesso a PCs, servidores e bancos de dados, de acordo com os Requisitos 3.1.2 a 3.1.9 do PA-DSS. **Clientes e revendedores/Integradores**: Estabelecer e manter IDs de usuário exclusivos e autenticação segura de acordo com o *Guia de Implementação do PA-DSS* e os Requisitos 3.1.2 a 3.1.10 do PA-DSS.
4.1	Implementar trilhas de auditoria automatizada.	▪ Definir as configurações de log em conformidade com o PCI DSS, de acordo com os Requisitos 4.2, 4.3 e 4.4 do PA-DSS. ▪ Os logs devem ser ativados, sua desabilitação resultará em não conformidade com o PCI DSS.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para uso de logs compatíveis, de acordo com os Requisitos 4.2, 4.3 e 4.4 do PA-DSS. **Clientes e revendedores/Integradores:** Estabelecer e manter logs compatíveis com o PCI DSS conforme o *Guia de Implementação do PA-DSS* e os Requisitos 4.2, 4.3 e 4.4 do PA-DSS.
4.4	Facilitar o registro centralizado.	Oferecer instruções e procedimentos para a incorporação dos logs do aplicativo de pagamento a um servidor de registro centralizado.	**Fornecedor de software**: Assegurar que o aplicativo de pagamento suporte o registro centralizado em ambientes de cliente conforme o Requisito 4.4 do PA-DSS. **Clientes e revendedores/Integradores:** Estabelecer e manter o registro centralizado de acordo com o *Guia de Implementação do PA-DSS* e do Requisito 4.4 do PA-DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
5.4	Usar somente serviços, protocolos, componentes, bem como softwares e hardwares dependentes que forem necessários e seguros, inclusive aqueles fornecidos por terceiros.	Documentar todos os protocolos, serviços, componentes, bem como softwares e hardwares dependentes exigidos, que forem necessários para qualquer funcionalidade do aplicativo de pagamento.	**Fornecedor de software:** Garanta que o aplicativo de pagamento ofereça suporte ao cliente para o uso somente de protocolos, serviços, etc. que forem seguros e necessários, ao 1) ter somente protocolos, serviços, etc. necessários estabelecidos como prontos para usar por padrão, 2) ter esses protocolos, serviços, etc. configurados com segurança por padrão e 3) documentar protocolos, serviços, etc. necessários como referência para clientes e revendedores/integradores. **Clientes e revendedores/Integradores:** Use a lista documentada do *Guia de Implementação* para garantir que somente protocolos, serviços, etc. necessários sejam usados no sistema, de acordo com o Requisito 5.4 do PA-DSS.
6.1	Implementação segura de tecnologia wireless.	Caso o wireless seja usado no ambiente de pagamento: ▪ Alterar ▪ Install a firewall: – Instalar um firewall entre quaisquer redes e sistemas wireless que armazenem dados de portadores de cartão e – Configurar esses firewalls para recusar ou controlar (se esse tráfego for necessário para fins comerciais) qualquer tráfego a partir do ambiente sem fio no ambiente de dados do portador do cartão.	**Fornecedor de software**: Orientar clientes e revendedores/integradores que se a tecnologia wireless for usada no aplicativo de pagamento, essas configurações padrão wireless do fornecedor deverão ser alteradas de acordo com o Requisito 2.1.1 do PCI DSS. **Clientes e revendedores/Integradores**: Para tecnologias wireless implementadas no ambiente de pagamento por clientes ou revendedores/integradores, instale um firewall de acordo com o Guia de Implementação do PA-DSS e o Requisito 2.1.1 do PCI DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
6.2	Proteger transmissões de dados do portador do cartão em redes wireless.	Caso o aplicativo de pagamento estiver implementado em um ambiente wireless, use as melhores práticas do setor (por exemplo, IEEE 802.11i) para implementar a criptografia robusta para autenticação e transmissão de dados do portador do cartão.	**Fornecedor de software**: Orientar clientes e revendedores/integradores que se a tecnologia wireless for usada com o aplicativo de pagamento, essas transmissões criptografadas seguras deverão ser implementadas de acordo com o Requisito 6.2 do PA-DSS. **Clientes e revendedores/Integradores**: Para tecnologias wireless implementadas no ambiente de pagamento por clientes ou revendedores/integradores, utilize transmissões criptografadas seguras, de acordo com o *Guia de Implementação do PA-DSS* e o Requisito 6.2 do PCI DSS.
9.1	Armazenar dados do portador do cartão somente em servidores não conectados à Internet.	Não armazenar dados do portador do cartão em sistemas acessíveis pela Internet (por exemplo, o servidor web e o servidor do banco de dados não deve estar no mesmo servidor).	**Fornecedor de software**: Garantir que o aplicativo de pagamento não requer armazenamento de dados no DMZ ou em sistemas acessíveis pela Internet e permitir o uso do DMZ de acordo com o Requisito 9 do PA-DSS. **Clientes e revendedores/Integradores**: Estabelecer e manter aplicativos de pagamento de modo que os dados do portador do cartão não sejam armazenados em sistemas acessíveis pela Internet, de acordo com o *Guia de Implementação do PA-DSS* e o Requisito 9 do PA-DSS
10.2	Implementar autenticação de dois fatores para acesso remoto ao aplicativo de pagamento.	Utilizar autenticação de dois fatores (ID de usuário e senha e um item de autenticação adicional, como um token) se o aplicativo de pagamento puder ser acessado remotamente.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para uso de autenticação de dois fatores, de acordo com o Requisito 10.2 do PA-DSS. **Clientes e revendedores/Integradores**: Estabelecer e manter autenticação de dois fatores para acesso remoto ao aplicativo de pagamento, de acordo com o *Guia de Implementação do PA-DSS* e o Requisito 8.3 do PA-DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
10.3.1	Oferecer com segurança atualizações remotas do aplicativo de pagamento.	▪ Ativar tecnologias de acesso remoto para atualizações do aplicativo de pagamento somente quando necessária para downloads e desligar imediatamente após a conclusão do download, conforme o Requisito 12.3.9 do PCI DSS ▪ Se o computador não estiver conectado via VPN ou outra conexão de alta velocidade, receber as atualizações remotas do aplicativo de pagamento por meio de um firewall configurado com segurança ou firewall pessoal, de acordo com o Requisito 1 ou 1.3.9 do PCI DSS.	**Fornecedor de software**: Oferecer com segurança atualizações remotas do aplicativo de pagamento. **Clientes e revendedores/Integradores**: Receber com segurança atualizações remotas do aplicativo de pagamento pelo fornecedor, de acordo com o Guia de Implementação do PA-DSS e os Requisitos 1, 1.3.9 e 12.3.9 do PCI DSS.
10.3.2	Implementar com segurança o acesso remoto ao software.	Implementar e usar os recursos de segurança do software de acesso remoto se o software for usado para acessar remotamente o aplicativo de pagamento ou seu ambiente.	**Fornecedor de software**: (1) Se o fornecedor usar produtos de acesso remoto para acessar sites do cliente, utilizar os recursos de segurança para acesso remoto como aqueles especificados no Requisito 10.3.2 **do PA-DSS. (2) Garantir que o aplicativo de pagamento ofereça suporte ao cliente para o uso de recursos de segurança para acesso remoto.** **Clientes e revendedores/Integradores**: Utilizar os recursos de segurança do acesso remoto se permitir o acesso remoto a aplicativos de pagamento, de acordo com o *Guia de implementação do PA-DSS* e o Requisito **11.3.b do PA-DSS**.
11.1	Proteger transmissões de dados do portador do cartão em redes públicas.	Implementar e usar criptografia robusta e protocolos de segurança para manter segura a transmissão de dados do portador do cartão em redes públicas.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para o uso de transmissões seguras de dados do portador do cartão em redes públicas, de acordo com o Requisito 11.1 do PA-DSS. **Clientes e revendedores/Integradores**: Estabelecer e manter transmissões seguras de dados do portador do cartão, de acordo com o *Guia de implementação do PA-DSS* e o Requisito 11.1 do PA-DSS.

PA-DSS Requisito	Tópico do PA-DSS	Conteúdo do Guia de Implementação	Responsabilidade da Implementação de controle
11.2	Criptografar dados do portador do cartão enviados por meio de tecnologias de envio de mensagens de usuário final.	Implementar e usar uma solução que converta o PAN ilegível ou implemente criptografia robusta caso os PANs possam ser enviados por tecnologias de mensagem do usuário final.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para criptografia de PANs, se enviados com tecnologias de envio de mensagens de usuário final, de acordo com o Requisito 11.2 do PA-DSS. **Clientes e revendedores/Integradores**: Criptografar todos os PANs enviados com tecnologias de envio de mensagens de usuário final, de acordo com o *Guia de implementação do PA-DSS* e o Requisito 11.2 do PA-DSS.
12.1	Criptografar os acessos administrativos não-console.	Implementar e usar criptografia robusta (como SSH, VPN ou SSL/TLS) para criptografia de qualquer acesso administrativo não-console ao aplicativo de pagamento ou servidores no ambiente de dados do portador do cartão.	**Fornecedor de software**: Garantir que o aplicativo de pagamento ofereça suporte ao cliente para criptografia de quer acesso administrativo não-console, de acordo com o Requisito 12.1 do PA-DSS. **Clientes e revendedores/Integradores**: Criptografar todos os acessos administrativos não-console, de acordo com o *Guia de implementação do PA-DSS* e o Requisito 12.1 do PA-DSS.

Apêndice B: Confirmação da configuração do laboratório de testes específico para a avaliação do PA-DSS

Para: *Fornecedor de Software Nome do Aplicativo Número da versão*

Para cada avaliação do PA-DSS conduzida, o PA-QSA deve preencher este documento para confirmar o status e as capacidades do laboratório usado para realizar o teste para a avaliação do PA-DSS. Este documento preenchido deve ser enviado junto com o documento *Requisitos e procedimentos de avaliação de segurança do PA-DSS*.

Para cada Procedimento de validação do laboratório, indique (usando as colunas "Concluído no laboratório do PA-QSA" ou "Concluído no laboratório do fornecedor") qual foi o laboratório usado para a avaliação e se laboratório que passou por esses Procedimentos de validação foi o laboratório do PA-QSA ou o do fornecedor do software.

Descreva a arquitetura e o ambiente do teste no laboratório no local para esta revisão do PA-DSS:

Descreva como o uso real do aplicativo de pagamento foi simulado no laboratório para esta revisão do PA-DSS:

Requisito do laboratório	Procedimento de validação do laboratório	Concluída em		Comentários
		Laboratório o PA-QSA	Laboratório Fornecedor	
1. Instalar o aplicativo de pagamento de acordo com as instruções de instalação do fornecedor ou o treinamento fornecido ao cliente.	**1.** Verificar se o manual de instalação do fornecedor ou o treinamento oferecido aos clientes foi utilizado para realizar a instalação padrão do produto do aplicativo de pagamento em todas as plataformas listadas no relatório do PA-DSS.	☐	☐	
2. Instalar e testar todas as versões do aplicativo de pagamento listadas no relatório do PA-DSS.	**2.a** Verificar se todas as implementações comuns (incluindo versões específicas de regiões/países) do aplicativo de pagamento a serem testadas foram instaladas.	☐	☐	
	2.b Verificar se todas as versões e plataformas do aplicativo de pagamento foram testadas.	☐	☐	
	2.c Verificar se todas as funcionalidades críticas do aplicativo de pagamento foram testadas.	☐	☐	

Requisito do laboratório	Procedimento de validação do laboratório	Concluída em		Comentários
		Laboratório PA-QSA	Laboratório Fornecedor	
3. Instalar e implementar todos os dispositivos de segurança necessários do PCI DSS.	**3.** Verificar se todos os dispositivos de segurança exigidos pelo PCI DSS (por exemplo, firewalls e software antivírus) foram implementados nos sistemas de teste.	☐	☐	
4. Instalar e/ou configurar todas as opções de segurança necessárias do PCI DSS.	**4.** Verificar todas as configurações do sistema, patches, etc. compatíveis com PCI DSS foram implementadas nos sistemas de teste para sistemas operacionais, software do sistema e aplicativos utilizados pelo aplicativo de pagamento.	☐	☐	
5. Simular o uso real do aplicativo de pagamento.	**5.a** O laboratório simula o uso real do aplicativo de pagamento, incluindo todos os sistemas e aplicativos onde o aplicativo está implementado. Por exemplo, uma implementação padrão do aplicativo de pagamento pode incluir um ambiente cliente/servidor dentro de uma loja de varejo com uma máquina POS e ou rede corporativa. O laboratório simula a implementação total.	☐	☐	
	5.b O laboratório utiliza somente números de cartão de teste para a simulação/teste — PANs ativos não são utilizados para testes. ***Observação:*** *Os cartões de teste geralmente podem ser obtidos com o fornecedor ou um processador ou adquirente.*	☐	☐	
	5.c O laboratório executa a autorização do aplicativo de pagamento e/ou funções de acordo e todos os resultados são examinados conforme o item 6, mais adiante.	☐	☐	
	5.d O laboratório e/ou processos mapeia todos os resultados produzidos pelo aplicativo de pagamento para cada situação possível, seja temporária, permanente, processamento de erro, modo de depuração, arquivos de log, etc.	☐	☐	
	5.e O laboratório e/ou processos simulam e validam todas as funções do aplicativo de pagamento, para incluir a geração de todos os erros e entradas de log usando dados reais simulados e inválidos.	☐	☐	

Requisito do laboratório	Procedimento de validação do laboratório	Concluída em		Comentários
		Laboratório PA-QSA	Laboratório Fornecedor	
6. Fornecer condições e uso de teste para as seguintes metodologias de teste de penetração:	**6.a Uso de ferramentas/métodos forenses:** Ferramentas/métodos forenses foram usados para pesquisar todos os resultados identificados para evidências de dados de autenticação confidenciais (ferramentas comerciais, scripts, etc.), conforme o Requisito 1.1.1–1.1.3 do PA-DSS.[4]	☐	☐	
	6.b Tentativa de explorar as vulnerabilidades do aplicativo: As vulnerabilidaes atuais (por exemplo, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.) foram usadas para tentar explorar o(s) aplicativo(s) de pagamento, de acordo com o Requisito 5.2 do PA-DSS.	☐	☐	
	6.c O laboratório e/ou processo tentou executar o código arbitrário durante o processo de atualização do aplicativo de pagamento: Execute o processo de atualização com código arbitrário conforme o requisito 7.2.b do PA-DSS.	☐	☐	
7. Utilizar o laboratório do fornecedor SOMENTE após verificar se todos os requisitos foram atendidos.	**7.a** Se o uso do laboratório do fornecedor de software for necessário (por exemplo, o PA-QSA não possui mainframe, AS400 ou Tandem o aplicativo de pagamento é executado ligado), o PA-QSA pode (1) usar o equipamento, sob empréstimo do fornecedor ou (2) usar as instalações do laboratório do fornecedor, contanto que isso seja detalhado no relatório junto com o local dos testes. Para cada opção, o PA-QSA verificou que o equipamento do fornecedor e o laboratório atendem aos seguintes requisitos:	☐	☐	
	7.b O PA-QSA verifica que o laboratório do fornecedor atende a todos os requisitos anteriores especificados neste documento e lista os detalhes no relatório.	☐	☐	

[4] Ferramenta ou método forense: Ferramenta ou método para descoberta, análise e apresentação de dados forenses, que fornece uma maneira robusta de autenticar, buscar e recuperar evidências do computador rápida e totalmente. No caso de ferramentas ou métodos forenses usados pelos PA-QSAs, essas ferramentas ou método devem localizar com precisão quaisquer dados de autenticação sensível gravados pelo aplicativo de pagamento. Essas ferramentas podem ser comerciais, de fonte aberta ou desenvolvidas internamente pelo PA-QSA.

Requisito do laboratório	Procedimento de validação do laboratório	Concluída em		Comentários
		Laboratório PA-QSA	Laboratório Fornecedor	
	7.c O PA-QSA deve validar a instalação simples do ambiente do laboratório para garantir que o ambiente simule com veracidade uma situação da vida real e que o fornecedor não tenha modificado ou falsificado o ambiente de qualquer maneira.	☐	☐	
	7.d Todos os testes são executados pelo PA-QSA (o fornecedor não pode executar testes em seu próprio aplicativo).	☐	☐	
	7.e Todos os testes são (1) realizados nas instalações do fornecedor ou (2) remotamente por meio de uma conexão de rede que usa um link seguro (por exemplo, VPN).	☐	☐	
	7.f Utilize somente números de cartão de teste para a simulação/teste — não utilize PANs ativos no teste. Esses cartões de teste geralmente podem ser obtidos com o fornecedor ou um processador ou adquirente.	☐	☐	
8. Mantenha um processo de controle de qualidade (QA) eficaz	**8.a** A equipe de QA do PA-QSA verifica se todas as plataformas identificadas no relatório do PA-DSS foram incluídas no teste.	☐	☐	
	8.b A equipe de QA do PA-QSA verifica se todos os requisitos do PA-DSS foram testados.	☐	☐	
	8.c A equipe de QA do PA-QSA verifica se as configurações e processos do laboratório do PA-QSA atendem aos requisitos e foram documentados com precisão no relatório.	☐	☐	
	8.d A equipe de QA do PA-QSA verifica se o relatório apresenta com precisão os resultados do teste.	☐	☐	